Finite Fixed Point Free Automorphism Groups

(Endliche fixpunktfreie Automorphismengruppen)

Diplomarbeit
zur Erlangung des akademischen Grades eines Diplom-Ingenieurs
in der Studienrichtung Technische Mathematik,
Stzw. Mathematik in den Naturwissenschaften

eingereicht von

Peter Mayr

Angefertigt am Institut für Algebra, Stochastik und
wissensbasierte mathematischen Systeme
der technisch-naturwissenschaftlichen Fakultät
der Johannes Kepler Universität Linz

bei

O.Univ.-Prof. Dr. Günter Pilz

Linz, im Dezember 1998

Vorwort

Ein berühmter Satz von Frobenius von 1901 zeigt, daß, wenn eine Gruppe G eine echte nicht triviale Untergruppe H besitzt, sodaß für alle $g \in G \setminus H$ gilt $H \cap g^{-1}Hg = \{1_G\}$, dann existiert eine normale Untergruppe N von G, sodaß G das halbdirekte Produkt von N und H darstellt. Gruppen mit dieser Eigenschaft - sogenannte Frobeniusgruppen - tauchen auf natürliche Art als transitive Permutationsgruppen auf, aber sie können auch als halbdirektes Produkt einer Gruppe N und einer auf N operierenden Automorphismengruppe, die als einzigen Fixpunkt das neutrale Element von N besitzt, betrachtet werden.

Nur wenig später, 1905, erhielt Dickson die ersten echten Fastkörper, indem er die Multiplikation in endlichen Körpern "störte". 1936 benutzte Zassenhaus die Tatsache, daß für alle Elemente a eines Rechtsfastkörpers N die Abbildungen $\lambda_a : x \mapsto ax$ mit der Fastkörpermultiplikation Automorphismen ohne nicht triviale Fixpunkte von $(N, +)$ darstellen. Dies ermöglichte ihm die Charakterisierung aller endlichen Fastkörper bis auf 7 Ausnahmen als Dickson-Fastkörper. Während die additive Gruppe eines endlichen Fastkörpers elementar abelsch ist, gelang es Thompson 1959 zu zeigen, daß jede Gruppe, die einen fixpunktfreien Automorphismus von Primzahlordnung besitzt, nilpotent ist.

Planare Fastringe $(N, +, \cdot)$ können als verallgemeinerte Fastkörper betrachtet werden, und Ferrero's Entdeckung, daß jeder planare Fastring aus einer additiven Gruppe und einer darauf operierenden fixpunktfreien Automorphismengruppe erzeugt werden kann, kommt nicht überraschend.

Im endlichen Fall können Frobeniusgruppen, Fastkörper und planare Fastringe als verschiedene Aspekte desselben gruppentheoretischen Konzepts interpretiert werden: als eine nilpotente Gruppe mit einer fixpunktfreien Automorphismengruppe. Diese Beziehungen werden in Kapitel 7 präsentiert.

Obwohl die Struktur von fixpunktfreien Automorphismengruppen bekannt ist, ist die Bestimmung einer solchen Gruppe Φ für eine beliebige nilpotente Gruppe G bei weitem nicht trivial. Das Ziel dieser Diplomarbeit ist es, den theoretischen Hintergrund darzustellen, wie man fixpunktfreie Automorphismengruppen konstruieren kann, und Funktionen zu bieten, um dies mit dem Computer auch wirklich zu tun. Das hauptsächliche Werkzeug dazu ist die Erweiterung von Gruppen. Nach Wiederholung der klassischen Resultate von Thompson und Zassenhaus in Kapitel 3, wobei auch neue und großteils elementare Beweise für die Charakterisation der auflösbaren fixpunktfreien Automorphismengruppen präsentiert werden, erfolgt eine schrittweise Annäherung an das Problem: der einfache Fall einer zyklischen Gruppe G ist in Kapitel 4 vollständig abgehandelt. Für elementar abelsche Gruppen erhalten wir ein Resultat von Ke und Kiechle aus 1993, das die zyklischen fixpunktfreien Automorphismengruppen Φ bestimmt, doch unter Verwendung eines anderen Zugangs. Dieser ermöglicht uns auch, den Fall der Quaternionengruppe zu lösen und sowohl für zyklische Φ als auch für Φ isomorph zu einer Quaternionengruppe einer bestimmten Grösse die Anzahl bis auf Konjugiertheit anzugeben. Weiters folgt eine zumindest teilweise Beschreibung der metazyklischen fixpunktfreien Automorphismengruppen, alles in Kapitel 5. Durch den Übergang von einer abelschen Gruppe G zu elementar abelschen Faktorgruppen in Kapitel 6 können alle vorhergehende Resultate verallgemeinert werden.

Schließlich stellt Kapitel 7 eine Implementation der ausgearbeiteten Ideen in dem Computer Algebra Programm GAP vor, die passende Werkzeuge zur Berechnung fixpunktfreier Automorphismengruppen einer breiteren Öffentlichkeit zugänglich machen soll. Beschreibungen von Funktionen und Beispiele schließen die Arbeit ab.

Preface

A famous theorem by Frobenius in 1901 proves that if a group G contains a proper non trivial subgroup H such that $H \cap g^{-1}Hg = \{1_G\}$ for all $g \in G \setminus H$, then there exists a normal subgroup N such that G is the semidirect product of N and H. Groups with this property - the so called Frobenius groups - arise in a natural way as transitive permutation groups, but they can also be characterized as semidirect product of a group N and a group of automorphisms H acting on N with the identity of N as single fixed point.

Only a short time later in 1905, Dickson obtained the first proper nearfields, when he "distorted" the multiplication in a finite field. In 1936, Zassenhaus made advance of the fact that for all elements a in a right nearfield N the mappings $\lambda_a : x \mapsto ax$ with nearfield multiplication are automorphisms without non trivial fixed points on $(N, +)$ and determined the structure of all finite fixed point free automorphism groups. This enabled him to characterize all finite nearfields as Dickson nearfields up to 7 exceptional cases. Whereas the additive group of a finite nearfield is elementary abelian, Thompson managed to show that any group which admits a fixed point free automorphism of prime order has to be nilpotent in 1959.

Planar nearrings $(N, +, \cdot)$ can be regarded as generalized nearfields and Ferrero's discovery that every planar nearring can be constructed from an additive group $(N, +)$ and a fixed point free automorphism group acting thereupon does not come as a surprise at all.

In the finite case Frobenius groups, nearfields and planar nearrings can be interpreted as different aspects of the same group theoretical concept: a nilpotent group with a fixed point free automorphism group. We present these interrelations in Chapter 7.

Although a lot is known about the structure of fixed point free automorphism groups in theory, the determination of such a group Φ for an arbitrary nilpotent group G is not trivial at all. The objective of this thesis is to give a theoretical setting how to construct fixed point free automorphism groups and to provide functions for actually doing this by computer. The main tool used in this computational context is extension. After revisiting the classical results from Thompson and Zassenhaus in Chapter 3, where we also present new and rather elementary proofs for the characterization of solvable fixed point free automorphism groups, we work our way up: the easy case of G being cyclic is completely dealt with in Chapter 4. For an elementary abelian group G we obtain a result from Ke and Kiechle, 1993, using a slightly different approach to present the cyclic fixed point free automorphism groups. This enables us to solve the quaternion case and to give the numbers for both cyclic and quaternion fixed point free automorphism groups Φ of a given size up to conjugation as well as a halfway description of metacyclic

Φ, all in Chapter 5. The transfer from an abelian group G to elementary abelian factor groups in Chapter 6 allows us to generalize all the preceding results.

Finally, Chapter 8 presents an implementation of the elaborated ideas in the computer algebra program GAP which should make convenient means for computation of fixed point free automorphism groups available to a broader community. Descriptions of functions and examples conclude the work.

Credits

I want to thank Günter Pilz for the supervision, support and personal encouragement of the work on this diploma thesis and the “Fonds zur Förderung der wissenschaftlichen Forschung” for financing it. Franz Binder provided helpful advice and Jürgen Ecker spent a lot of time discussing theoretical and computational aspects of this matter with me. I am also indebted to him for a first look at this document and some corrections and suggestions to make it more readable.

I owe a great deal to several persons, my friends and my parents, for enduring me at almost any time but as up to them I would wish to express my thankfulness personally.

Contents

Vorwort i

Preface iii

Credits v

Chapter 1. Introduction: Group Theory 1
1. Homomorphisms and Normal Subgroups 1
2. Sylow Theorems 3
3. Products of Groups 3
4. Structure of Finite Abelian Groups 4
5. Automorphism Group of Cyclic Groups 4
6. Solvable Groups 6
7. Nilpotent Groups 7
8. Special Types of Finite p-Groups 7
9. Quaternion groups 7
10. Frattini Subgroup 9
11. Linear Groups 9
12. The Schur Zassenhaus Theorem 9
13. Applications of the Transfer 9

Chapter 2. Introduction: Modules and Vector Spaces 11
1. Linear Transformations 11
2. Rational Canonical Form 13
3. Polynomials over Finite Fields 16

Chapter 3. Structure of Fixed Point Free Automorphism Groups 17
1. Necessary Conditions on G and Φ 17
2. Characterization of Φ 20

Chapter 4. The Cyclic Case 31

Chapter 5. The Elementary Abelian Case 33
1. Cyclic Φ 33
2. Quaternion Φ 40
3. Φ of Type (I) 47

Chapter 6. The Abelian Case 49
1. Transfer to the Elementary Abelian Case 49
2. Cyclic Φ 56
3. Quaternion Φ 59
4. Φ of type (I) 60

Chapter 7. Applications of Fixed Point Free Automorphism Groups 61
1. Frobenius Groups 61
2. Planar Nearrings 63
3. Finite Nearfields 65

Chapter 8. An Implementation in GAP4 67
1. Preliminaries 67
2. Defining Groups in GAP 68
3. Computation of Fixed Point Free Automorphism Groups 69

Chapter 9. Examples of Special Fixed Point Free Automorphism Groups 75
1. Groups of Order 64 75
2. The Elementary Abelian Group of Order 121 77
3. An Abelian Example 78

Lebenslauf 79

Bibliography 81

Index 83

CHAPTER 1

Introduction: Group Theory

In this first chapter we introduce the concepts of group theory, which we are concerned with. We will not give a complete account of basic group theory and we will also not prove every result cited (see e.g. [**Hup67**], [**Rob96**]) but just collect properties we need in the following.

Throughout this thesis let all groups be finite.

1. Homomorphisms and Normal Subgroups

1.1. Definition. Let G and H be groups. A function $\alpha : G \to H$ is called a *homomorphism* if

$$\alpha(xy) = \alpha(x)\alpha(y)$$

for all $x, y \in G$. The set of all homomorphisms from G to H is denoted by

$$\mathrm{Hom}(G, H).$$

A homorphism $\alpha : G \to G$ is called an *endomorphism* of G and we write

$$\mathrm{End}(G) = \mathrm{Hom}(G, G).$$

Let 1_G denote the identity of the group G and id_G the identity function $\mathrm{id}_G : G \to G, x \mapsto x$. Clearly id_G and the function $h : G \to G, x \mapsto 1_G$ are endomorphisms.

1.2. Definition. For a homomorphism $\alpha : G \to H$ we define the *image* $\mathrm{Im}\,\alpha$ and the *kernel* $\mathrm{Ker}\,\alpha$ as follows

$$\mathrm{Im}\,\alpha = \{\alpha(x) : x \in G\} = \alpha(G)$$

and

$$\mathrm{Ker}\,\alpha = \{x \in G : \alpha(x) = 1_H\}.$$

1.3. Definition. An injective (or one-one) homomorphism is called a *monomorphism* and a surjective (or onto) homomorphism an *epimorphism* : a bijective homomorphism we call an *isomorphism* . For a group G an *automorphism* of G is an isomorphism from G to G. The set of automorphisms of G is denoted by

$$\mathrm{Aut}(G).$$

1.4. Definition. Let $x, g \in G$ and write

$$x^g = g^{-1}xg.$$

This element is called the *conjugate* of x by g. The function $\tau_g : G \to G$ with $\tau_g : x \mapsto x^g$ is called the *inner automorphism* of G induced by g and we write

$$\mathrm{Inn}(G)$$

for the set of all inner automorphisms on G .

$\operatorname{Aut}(G)$ is a group with respect to functional composition and $\operatorname{Inn}(G)$ is a subgroup thereof.

1.5. Definition. A subgroup H of G, $H \leq G$, is called:

(a) *normal* iff $\alpha(H) = H$ for all $\alpha \in \operatorname{Inn}(G)$, written $H \lhd G$;
(b) *characteristic* iff $\alpha(H) = H$ for all $\alpha \in \operatorname{Aut}(G)$;
(c) *fully-invariant* iff $\alpha(H) \leq H$ for all $\alpha \in \operatorname{End}(G)$.

1.6. Theorem (First Isomorphism Theorem). Let $\alpha : G \to H$ be a group homomorphism. Then

$$G/\operatorname{Ker}\alpha \cong \operatorname{Im}\alpha.$$

($\cong$ means is isomorphic to.)

Proof. For $n, m \in \operatorname{Ker}\alpha$ it holds that $\alpha(nm^{-1}) = \alpha(n)\alpha(m)^{-1} = 1_G$ and thus $\operatorname{Ker}\alpha$ is a subgroup of G. Furthermore, $\alpha(g^{-1}ng) = \alpha(g)^{-1}\alpha(n)\alpha(g) = 1_G$ for any $g \in G$ and $\operatorname{Ker}\alpha \lhd G$.

We define a mapping

$$h : x \cdot \operatorname{Ker}\alpha \mapsto \alpha(x)$$

which is well-defined since $\alpha(xn) = \alpha(x)$ for each $n \in \operatorname{Ker}\alpha$ and it clearly is an epimorphism. Now $x \cdot \operatorname{Ker}\alpha$ and $y \cdot \operatorname{Ker}\alpha$ are mapped to the same element $\alpha(x) = \alpha(y)$ if and only if $\alpha(xy^{-1}) = 1_H$, which means $x \cdot \operatorname{Ker}\alpha = y \cdot \operatorname{Ker}\alpha$; thus h is an isomorphism. □

1.7. Definition. Let X be a nonempty subset of a group G.

$$C_G(X) = \{g \in G : xg = gx, \forall x \in X\}$$

is called the *centralizer* of X in G and for $X = G$ we write $C(G)$ for the *center* of G.

$$N_G(X) = \{g \in G : g^{-1}Xg = X\}$$

is called the *normalizer* of X in G.

$C_G(X)$ and $N_G(X)$ are subgroups of G. If $X \leq G$, then $N_G(X)$ is the largest subgroup of G in which X is normal.

1.8. Proposition. Let H be a subgroup of a group G. Then

$$C_G(H) \lhd N_G(H)$$

and $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\operatorname{Aut}(H)$.

Proof. Clearly $C_G(H) \leq N_G(H)$. For $g \in N_G(H)$ let τ_g denote the function $h \mapsto g^{-1}hg$. Evidently, τ_g is an automorphism on H and

$$\begin{array}{rcl} \tau : N_G(H) & \to & \operatorname{Aut}(H), \\ g & \mapsto & \tau_g \end{array}$$

is a homomorphism with kernel $C_G(H)$. Thus $C_G(H)$ is normal in $N_G(H)$ and by the First Isomorphism Theorem 1.6, the factor group $N_G(H)/C_G(H)$ can be embedded into $\operatorname{Aut}(H)$. □

We are not interested in $\operatorname{Aut}(G)$ as a whole but in subgroups $\Phi \leq \operatorname{Aut}(G)$, which operate on G without non trivial fixed points.

1.9. Definition. An automorphism α of a group G is said to have a *fixed point g* in G if $\alpha(g) = g$. If 1_G is the only fixed point of α, then α is called *fixed point free* on G. A subgroup Φ of $\operatorname{Aut}(G)$ is said to be *fixed point free* on G if every element φ in $\Phi \setminus \{\mathrm{id}_G\}$ is fixed point free.

Obviously, every inner automorphism $\tau_x \in \operatorname{Inn}(G)$ has a fixed point, namely x. We are ready for our first example of a fixed point free automorphism group:

1.10. Example. Consider the additive group $(Z_7, +)$ and let $i : Z_7 \to Z_7$ denote the mapping $x \mapsto -x$. Evidently, $i(x+y) = -(x+y) = -y-x = -x-y = i(x)+i(y)$ and $i(x) = 0$ implies $x = 0$. Thus i is an automorphism. Suppose there is $x \in Z_7$ such that $i(x) = x$, that is, $x = -x$, then $x = 0$. So i is fixed point free.

The automorphism group generated by i is $\langle i \rangle = \{\mathrm{id}, i\}$ and every non trivial element therein is fixed point free way on Z_7.

2. Sylow Theorems

1.11. Definition.

(a) If p is a prime, a finite group G is a *p-group* if $|G| = p^n$ for some $n \geq 1$.
(b) H is a *p-subgroup* of a group G if $H \leq G$ and H is a p-group.
(c) Let G be an arbitrary finite group, p a prime and p^n the highest power of p dividing $|G|$. Then H is a *p-Sylow subgroup* of G if $H \leq G$ and $|H| = p^n$.

1.12. Proposition. A non trivial finite p-group has a non trivial center.

Proof. This is a simple application of the class equation, see [**Rob96**], p.39. □

1.13. Theorem (Sylow). Let G be a finite group and let p be a prime.

(a) G has a p-Sylow subgroup and furthermore every p-subgroup is contained in some p-Sylow subgroup.
(b) The p-Sylow subgroups of G are mutually conjugate.
(c) The number of p-Sylow subgroups of G is congruent to 1 mod p and divides G.

Proof. see [**Rob96**], p.39. □

3. Products of Groups

1.14. Definition. Let $N \lhd G$. If there is $H \leq G$ such that $G = HN$ and $H \cap N = 1_G$, then H is called a *complement* of N in G and G is said to be the *semidirect product* of N and H, written as

$$G = H \ltimes N.$$

If $H \lhd G$, then G is called the *direct product* of N and H, in symbols

$$G = H \times N$$

For direct products of additive groups we use the notation $G = H \oplus N$.

1.15. Proposition. ([**Hup67**] (I. 9.4)) Let $G = G_1 \times \cdots \times G_m$ be the direct product of its p_i-Sylow subgroups G_i with p_i prime for $1 \leq i \leq m$. Then

$$\operatorname{Aut}(G) \cong \operatorname{Aut}(G_1) \times \cdots \times \operatorname{Aut}(G_m).$$

Proof. For each prime p_i, the direct factor G_i is the only p_i-Sylow subgroup of G and therefore characteristic. For every automorphism $\alpha \in \mathrm{Aut}(G)$, we have $\alpha(G_i) = G_i$ for $i = 1, \ldots, m$.

Let $\alpha_i := \alpha|_{G_i}$ denote the restriction of α on G_i. Obviously, the mapping

$$\begin{array}{rcl} h : \mathrm{Aut}(G) & \rightarrow & \mathrm{Aut}(G_1) \times \cdots \times \mathrm{Aut}(G_m) \\ \alpha & \mapsto & (\alpha_1, \ldots, \alpha_m) \end{array}$$

is a monomorphism. On the other hand, each tuple $(\alpha_1, \ldots, \alpha_m) \in \mathrm{Aut}(G_1) \times \cdots \times \mathrm{Aut}(G_m)$ defines an automorphism α on $G_1 \times \cdots \times G_m$ via

$$\alpha(g_1, \ldots, g_m) := (\alpha_1(g_1), \ldots, \alpha_m(g_m)),$$

where $g_i \in G_i$ for $i = 1, \ldots, m$. Thus $\mathrm{Aut}(G) \cong \mathrm{Aut}(G_1) \times \cdots \times \mathrm{Aut}(G_m)$. □

4. Structure of Finite Abelian Groups

We go on to finite abelian groups which are characterized by the following:

1.16. Theorem (Main Theorem on Finite Abelian Groups). Let G be a finite abelian group. Then there are $g_i \in G$ such that $G = \bigoplus_{i=1}^{m} \langle g_i \rangle$ with $\mathrm{ord}(g_i) = p_i^{d_i}$ and p_i prime for $i = 1, \ldots, m$. The prime powers $p_i^{d_i}$ are uniquely determined by G and conversely they determine G up to isomorphism. The $p_i^{d_i}$ are called the *abelian invariants* of G.

Proof. see [**Hup67**], p. 80, [**Rob96**], p. 102. □

5. Automorphism Group of Cyclic Groups

Z_n^* denotes the *multiplicative group of units* of the ring $(Z_n, +, \cdot)$, i.e., the group of all elements which have a multiplicative inverse in Z_n.

1.17. Proposition. Let G be a cyclic group of finite order n. Then $\mathrm{Aut}(G)$ consists of all automorphisms $\alpha_l : g \mapsto g^l$ where $1 \leq l \leq n$ and $\gcd(l, n) = 1$; moreover, the mapping $l + nZ \mapsto \alpha_l$ is an isomorphism from Z_n^* to $\mathrm{Aut}(G)$. In particular, $\mathrm{Aut}(G)$ is abelian and has order $\phi(n)$, where ϕ denotes *Euler's function* .

Proof. Let $G = \langle x \rangle$ and let $\alpha \in \mathrm{Aut}(G)$. Since

$$\alpha(x^i) = \alpha(x)^i$$

for $1 \leq i \leq n$, the automorphism α is completely determined by $\alpha(x) = x^l$. Evidently,

$$n = \mathrm{ord}(x) = \mathrm{ord}(x^l) = n / \gcd(n, l)$$

and l is relatively prime to n.

Conversely, for each integer l such that $\gcd(n, l) = 1$ the mapping $g \mapsto g^l$ for $g \in G$ is an automorphism. The rest is clear. □

The investigation of these groups Z_n^* in general will pay off later on.

1.18. Proposition. (**[Hup67]** (I. 13.19b))

(a) If $n = \prod_{i=1}^r n_i$ where $\gcd(n_i, n_j) = 1$ for $i \neq j$, then

$$Z_n^* = \bigoplus_{i=1}^r Z_{n_i}^*.$$

(b) $Z_{p^d}^*$ with p an odd prime is cyclic.

(c) $Z_{2^d}^*$ with $d \geq 2$ is isomorphic to $Z_{2^{d-2}} \oplus Z_2$.

Proof.

(a) Z_n^* is isomorphic to $\mathrm{Aut}(G)$ where G is a cyclic group of order n by Proposition 1.17. Theorem 1.16 provides a decomposition

$$G = \bigoplus_{i=1}^r G_i$$

with $|G_i| = n_i$ and $\gcd(n_i, n_j) = 1$ for $i \neq j$. Thus

$$\mathrm{Aut}(G) \cong \bigoplus_{i=1}^r \mathrm{Aut}(G_i)$$

by Proposition 1.15.

(b) The mapping

$$\begin{array}{rcl} h : Z_{p^d}^* & \to & Z_p^* \\ x + p^d Z & \mapsto & x + pZ. \end{array}$$

is an epimorphism with

$$\mathrm{Ker}\, h = \{x + p^d Z : x \equiv 1 \bmod p\}$$

and $|\mathrm{Ker}\, h| = p^{d-1}$. We show $\mathrm{Ker}\, h$ to be cyclic by verifying that $1+p+p^dZ$ is of order p^{d-1} in $Z_{p^d}^*$.

For $p > 2, t \geq 0$, there is some $l \in Z$ such that

$$(1+p)^{p^t} = 1 + p^{t+1} + lp^{t+2}.$$

The hypothesis is true for $t = 0$, now assume it holds for t and we prove it for $t+1$.

$$\begin{aligned} (1+p)^{p^{t+1}} &= ((1+p)^{p^t})^p \\ &= (1 + p^{t+1} + lp^{t+2})^p \\ &= \sum_{i=0}^p \binom{p}{i} (p^{t+1} + lp^{t+2})^i \\ &= 1 + p(p^{t+1} + lp^{t+2}) + \sum_{i=2}^p \binom{p}{i} p^{(t+1)i} (1+lp)^i. \end{aligned}$$

Since p is a divisor of $\binom{p}{i}$ for $0 < i < p$, we obtain that p^{t+3} divides $\sum_{i=2}^p \binom{p}{i} p^{(t+1)i}(1+lp)^i$ and finally

$$(1+p)^{p^{t+1}} = 1 + p^{t+2} + l' p^{t+3}$$

for some integer l' and the assertion is proven. Now

$$(1+p)^{p^{d-2}} = 1 + p^{d-1} \neq 1 \bmod p^d,$$

the order of $1+p$ in $Z^*_{p^d}$ is p^{d-1} indeed and $\operatorname{Ker} h$ is cyclic.

$Z^*_{p^d}$ is abelian and thus the direct product of cyclic groups of prime power order by Theorem 1.16. Let

$$Z^*_{p^d} = \langle g_1 \rangle \oplus \cdots \oplus \langle g_r \rangle \oplus \operatorname{Ker} h$$

be a decomposition with $\gcd(\langle g_i \rangle, p) = 1$ for $1 \leq i \leq r$. Then

$$Z^*_{p^d} / \operatorname{Ker} h \cong \langle g_1 \rangle \oplus \cdots \oplus \langle g_r \rangle \cong \operatorname{Im} h = Z^*_p.$$

Z^*_p is cyclic since the prime remainders mod p form a field. Thus $Z^*_{p^d}$ is the direct product of cyclic groups of relatively prime orders $p-1$ and p^{d-1}. Therefore $Z^*_{p^d}$ is cyclic itself.

(c) The proof of (c) is an analog to the proof for (b) where we use a mapping

$$\begin{aligned} h : Z^*_{2^d} &\to Z^*_4 \\ x + 2^d Z &\mapsto x + 4Z. \end{aligned}$$

and verify that $\operatorname{Ker} h$ is cyclic.

□

6. Solvable Groups

1.19. Definition. A group G is said to be *solvable* if it has a series

$$\{1_G\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

in which each factor G_{i+1}/G_i is abelian.

Solvability can also be characterized by using a particular series which we introduce now.

1.20. Definition. For a, b elements of the group G we call

$$[a, b] = a^{-1} b^{-1} a b$$

the *commutator* of a and b. The subgroup of G generated by all of the commutators in G is denoted by

$$G' = \langle [a, b] : a, b \in G \rangle,$$

and called the *derived subgroup* of G. By recursion, we define $G^{(i+1)}$ as the derived subgroup of $G^{(i)}$ with $G^{(0)} = G$,

$$G^{(i+1)} = (G^{(i)})'$$

We also write $G^{(2)} = G''$ and $G^{(3)} = G'''$.

Evidently, $G \geq G' \geq G'' \geq G''' \geq \ldots$ and all $G^{(i)}$ are characteristic subgroups of G. Each factor G_{i+1}/G_i is abelian. A group G is solvable if and only if $G^{(l)} = \{1_G\}$ for some l.

1.21. Definition. A group G is called *perfect* if $G = G'$.

7. Nilpotent Groups

1.22. Definition. A group G is called *nilpotent* if it has a series

$$\{1_G\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

such that G_{i+1}/G_i is contained in the center of G/G_i for all i.

Note that by definition a nilpotent group G has a non trivial center. Also, every nilpotent group is solvable. There are several group theoretical properties which are equivalent to nilpotence for finite groups. We give the formulations which are most useful for our purposes.

1.23. Theorem. Let G be a finite group. Then the following are equivalent:

(a) G is nilpotent;
(b) every maximal subgroup of G is normal;
(c) G is the direct product of its Sylow subgroups.

Proof. see [**Rob96**], p. 130. □

8. Special Types of Finite p-Groups

1.24. Theorem. A group of order p^{t+1} has a cyclic maximal subgroup of order p^t if and only if it is of one of the following types:

(a) a cyclic group of order p^{t+1};
(b) the direct product of a cyclic group of order p^t and one of order p;
(c) $\langle a, b : a^{p^{n-1}} = b^p = 1, b^{-1}ab = a^{1+p^{n-2}}\rangle$ for $t \geq 2$;
(d) the *dihedral group* $D_{2^{t+1}} = \langle a, b : a^{2^t} = b^2 = 1, b^{-1}ab = a^{-1}\rangle$ for $t \geq 2$;
(e) the *generalized quaternion group* $Q_{2^{t+1}} = \langle a, b : a^{2^t} = 1, b^2 = a^{2^{t-1}}, b^{-1}ab = a^{-1}\rangle$ for $t \geq 2$;
(f) the *semidihedral group* $\langle a, b : a^{2^t} = b^2 = 1, b^{-1}ab = a^{-1+2^{t-1}}\rangle$ for $t \geq 2$.

Proof. see [**Rob96**], p. 141. □

1.25. Theorem. A finite p-group has exactly one subgroup of order p if and only if it is cyclic or a generalized quaternion group.

Proof. see [**Rob96**], p. 143. □

9. Quaternion groups

Since the generalized quaternion groups occupy such a central position, we investigate them in detail. The propositions given in this section are rather elementary and can be found at least partly as exercises in books on basic group theory, see e.g. [**Hup67**], p.93-94, or see [**Wäh87**], p.311-312, for a summary of even more properties.

1.26. Proposition. Let $Q_{2^{t+1}}$ be the quaternion group of order 2^{t+1} with the presentation

$$Q_{2^{t+1}} = \langle a, b : a^{2^t} = 1, b^2 = a^{2^{t-1}}, b^{-1}ab = a^{-1}\rangle.$$

Then

(a) every element of $Q_{2^{t+1}}$ can be written uniquely in the form $b^i a^j$ with $0 \leq i < 2$ and $0 \leq j < 2^t$;
(b) $Q'_{2^{t+1}} = \langle a^2\rangle$;

(c) $C(Q_{2^{t+1}}) = \langle b^2 \rangle$ and b^2 is the only element of order 2 in $Q_{2^{t+1}}$.

PROOF. This follows immediately from the relations for the generators of $Q_{2^{t+1}}$. □

For the following, we have to distinguish between $t = 2$ and $t > 2$.

1.27. Proposition.

(a) Every proper subgroup of Q_8 is cyclic and a normal subgroup.
(b) $|\operatorname{Aut}(Q_8)| = 24$.

PROOF. (a) By Proposition 1.26, there is exactly one element b^2 of order 2 in G and $\langle b^2 \rangle = C(Q_8)$. The subgroups of order 4 are given by $\langle a \rangle, \langle b \rangle, \langle ba \rangle$. Since each of them has index 2 in Q_8, they are normal.

(b) Q_8 has 6 elements of order 4, namely $S = \{a, a^{-1}, b, b^{-1}, ba, ba^{-1}\}$. Any two distinct elements $x, y \in S$ with $x \neq y^{-1}$ generate the whole group Q_8 and also fulfill the relations $x^2 = y^2$ and $xy = yx$. Therefore the mapping $h : a \mapsto x, b \mapsto y$ is an automorphism. There are 6 possibilities to choose x and once the image of a is fixed, 4 possibilities remain to choose y. Thus $|\operatorname{Aut}(Q_8)| = 24$.

□

1.28. Proposition. Let $Q_{2^{t+1}} = \langle a, b : a^{2^t} = 1, b^2 = a^{2^{t-1}}, b^{-1}ab = a^{-1} \rangle$ for $t \geq 3$.

(a) Every element in $Q_{2^{t+1}} \setminus \langle a \rangle$ is of order 4.
(b) $\langle a \rangle$ is the only cyclic subgroup of index 2 in $Q_{2^{t+1}}$.
(c) Every proper subgroup of $Q_{2^{t+1}}$ is cyclic or a quaternion group.
(d) $\operatorname{Aut}(Q_{2^{t+1}})$ is a 2-group.

PROOF. (a) The elements of $Q_{2^{t+1}} \setminus \langle a \rangle$ are precisely of the form ba^i for $0 \leq i < 2^t$. Since $ab = ba^{-1}$, we have

$$(ba^i)^2 = ba^iba^i = bba^{-i}a^i = b^2$$

and ba^i is of order 4.

(b) By (a).

(c) Let H be a subgroup of $Q_{2^{t+1}}$. If $H \leq \langle a \rangle$, then H is cyclic. If $ba^j \in H \setminus \langle a \rangle$ and $\langle a^i \rangle = H \cap \langle a \rangle$, then $\langle a, H \rangle = Q_{2^{t+1}}$ and

$$\frac{|H|}{|\langle a \rangle \cap H|} = \frac{|\langle a, H \rangle|}{|\langle a \rangle|} = 2$$

$\langle a^i, ba^j \rangle$ is of order $2 \cdot |\langle a \rangle \cap H|$ and thus equal to H. Now H is either cyclic of order 4 if $a^i = b^2$ or H is a quaternion group if $a^i \neq b^2$.

(d) $Q_{2^{t+1}}$ has 2^{t-1} elements of order 2^t, namely a^i for $\gcd(i, 2) = 1$ and $0 < i < 2^t$ and there are 2^t elements $ba^j \in Q_{2^{t+1}} \setminus \langle a \rangle$ of order 4 for $0 \leq j < 2^t$. Any pair $x = a^i, y = ba^j$ generates the whole group $Q_{2^{t+1}}$ and fulfills the relations $x^{2^{t-1}} = y^2$ as well as as $y^{-1}xy = x^{-1}$. Thus the mapping $h : a \mapsto x, b \mapsto y$ is an automorphism of the group and there are $|\operatorname{Aut}(Q_{2^{t+1}})| = 2^{t-1} * 2^t$ automorphisms in total.

□

10. Frattini Subgroup

1.29. Definition. The *Frattini subgroup* of an arbitrary finite group G is defined to be the intersection of all the maximal subgroups and denoted by $F(G)$.

This subgroup $F(G)$ is characteristic and it has the remarkable property that every element $f \in F(G)$ can be canceled from each set of generators of G:

1.30. Theorem. For any group G, an element $f \in G$ is in $F(G)$, if and only if $G = \langle g, X \rangle$ always implies that $G = \langle X \rangle$, where $X \subseteq G$.

Proof. see [**Rob96**], p.135. □

11. Linear Groups

Groups of matrices provide a variety of interesting examples.

Let F be a field and let $\mathrm{GL}(n, F)$ denote the set of all $n \times n$ matrices with coefficients in F which have inverses. Taking matrix multiplication as the group operation it can be seen that $\mathrm{GL}(n, F)$ is a group with identity element I, the $n \times n$ identity matrix.

Let $\mathrm{SL}(n, F)$ denote the set of all $n \times n$ matrices over F with determinant equal to $1 \in F$. Because of the multiplicativity of det, this is a subgroup of $\mathrm{GL}(n, F)$.

1.31. Definition. $\mathrm{GL}(n, F)$ is called the *general linear group* of degree n over F. $\mathrm{SL}(n, F)$ is called the *special linear group* of degree n over F.

If F is a finite field of order $|F| = p^f$, then we also write $\mathrm{GL}(n, p^f)$ and $\mathrm{SL}(n, p^f)$, respectively. While we do not want to deal with linear groups in general, we have to stress a particular example.

1.32. Theorem. Let $G = \mathrm{SL}(2, 5)$. Then G has the following properties:

(a) $|G| = 120$.
(b) There is exactly 1 element of order 2 in G, namely $-I$, the negative identity matrix, and $C(G) = \langle -I \rangle$.
(c) $G' = G$, and in particular G is not solvable.
(d) $\langle -I \rangle$ is the only nontrivial normal subgroup of G.
(e) $G \simeq \langle a, b, c : a^3 = b^5 = c^2 = 1, c^{-1}ac = a, c^{-1}bc = b, (ab)^2 = c \rangle$

Proof. see [**Wäh87**], p.317. □

12. The Schur Zassenhaus Theorem

Another fundamental group theoretical result will be used by us later on.

1.33. Theorem (Schur, Zassenhaus). Let N be a normal subgroup of a finite group G. Assume that $|N|$ and $|G/N|$ are relatively prime. Then G contains subgroups of order $|G/N|$ and any two of them are conjugate in G.

Proof. see [**Rob96**], p. 253. □

13. Applications of the Transfer

Since we do not want to present the transfer homomorphism, we choose formulations which avoid its special terminology. However, it is the underlying technique for the proof of the following two theorems. To get acquainted with the transfer and other theorems depending on it, we recommend [**Rob96**].

1.34. Theorem (Burnside). Let P be a p-Sylow subgroup of G and $N_G(P) = C_G(P)$. Then there is a normal subgroup N of G with $G/N \cong P$.

Proof. see [**Hup67**], p.419, [**Rob96**], p.289. □

1.35. Theorem (Grüns First Theorem). Let G be a finite group and let P be a p-Sylow subgroup of G. If $N = N_G(P)$, then

$$P \cap G' = \langle P \cap N', P \cap g^{-1}P'g : g \in G \rangle.$$

Proof. see [**Rob96**], p.292. □

CHAPTER 2

Introduction: Modules and Vector Spaces

Regular linear transformations on vector spaces occur quite naturally in the subject as they correspond to automorphisms on elementary abelian groups. Moreover, they are particularly accessible since there exist various normal forms in which they can be expressed. Our objective is to obtain the rational canonical form for linear transformations, which we will need later on in Chapter 5. It is only for its development that we use module theory and here we concentrate on selected results without giving proofs. For a detailed account of the matter in its own, we refer to [**AW92**].

The properties of finite fields and polynomials thereupon have been taken from [**LN84**].

1. Linear Transformations

2.1. Definition. Let R be ring (not necessarily commutative) with identity 1. A *left R-module* is an abelian group M together with a scalar multiplication map

$$\cdot : R \times M \to M$$

that satisfy the following axioms (as is customary, we let M be an additive group with operation $+$ and write am for the scalar multiplication of $m \in M$ by $a \in R$). Let $a, b \in R$ and $m, n \in M$.

(a) $a(m+n) = am + an$.
(b) $(a+b)m = am + bm$.
(c) $(ab)m = a(bm)$.
(d) $1m = m$.

We can define a right module by making the obvious modifications.

2.2. Definition. Let R be a ring and let M and N be R-modules. A function $f : M \to N$ is an *R-module homomorphism* if for all $m_1, m_2 \in M$ and $a \in R$

(a) $f(m_1 + m_2) = f(m_1) + f(m_2)$,
(b) $f(am) = af(m)$.

The set of all R-module homomorphisms from M to N will be denoted by $\mathrm{Hom}_R(M, N)$. In case $M = N$ we write $\mathrm{End}_R(M)$.

2.3. Definition. If R is a ring, M is an R-module, and X is a subset of M, then the *annihilator* of X, denoted $\mathrm{Ann}(X)$ is defined by

$$\mathrm{Ann}(X) = \{a \in R : ax = 0 \text{ for all } x \in X\}$$

2.4. Definition. Let R be an integral domain and let M be an R-module. An element $x \in M$ is called a *torsion element* if $\mathrm{Ann}(x) \neq \{0\}$. If all elements of M are torsion, then M is said to be *torsion* .

2.5. Definition.

(a) Let F be a field. Then an F-module V is called a *vector space* over F.

(b) If V and W are vector spaces over the field F, then a *linear transformation* from V to W is an F-module homomorphism from V to W.

2.6. Proposition. Let $(G, +)$ be an elementary abelian group of order p^n and let F_p denote the field of order p. Then G is a vector space over F_p with the scalar multiplication

$$ag = \begin{cases} g + \ldots + g & (a \text{ terms}) \text{ if } a \neq 0_F \\ 0_G & \text{if } a = 0_F \end{cases}$$

and the endomorphisms of G are F_p-module endomorphisms.

Proof. Since G is abelian, this is easily seen by checking the F_p-module axioms. □

2.7. Definition. Let V be an n-dimensional vector space over the field F and let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be a basis of V, i.e., each element $v \in V$ has a representation $v = a_1 v_1 + \cdots + a_n v_n$, where the $a_i \in F$ for $1 \leq i \leq n$ are uniquely determined. For each $T \in \mathrm{End}_F(V)$ we define the matrix of T with respect to $\mathcal{B}$ by

$$[T]_{\mathcal{B}} = A$$

with $A = (a_{ij})$ and $T(v_j) = a_{1j} v_1 + \cdots + a_{nj} v_n$.

It is clear from the construction that for a fixed basis $\mathcal{B}$ every $n \times n$ matrix A over F is the matrix $[T]_{\mathcal{B}}$ for a unique $T \in \mathrm{End}_F(V)$.

Let $\mathrm{Aut}_F(V)$ denote the set of bijective F-homomorphisms from the vector space V over F into V. Then $\mathrm{Aut}_F(V)$ is a group.

2.8. Proposition. Let V be an n-dimensional vector space over the field F. Then $\mathrm{Aut}_F(V)$ and $GL(n, F)$ are isomorphic as groups.

Proof. Let $\mathcal{B}$ be a basis of V. The mapping h :

$$\begin{array}{ccc} \mathrm{Aut}_F(V) & \rightarrow & GL(n, F) \\ T & \mapsto & [T]_{\mathcal{B}} \end{array}$$

is a bijection. Let $S, T \in \mathrm{Aut}_F(V)$ with $[S]_{\mathcal{B}} = A$ and $[T]_{\mathcal{B}} = B$. Since

$$S(T(v)) = ABv$$

implies $[ST]_{\mathcal{B}} = AB$, we identify h as an isomorphism. □

Now we transfer the concept of being fixed point free from automorphisms on groups to regular linear transformations of vector spaces.

2.9. Definition. Let T be a linear transformation on the vector space V over the field F. A nonzero vector $v \in V$ is called an *eigenvector* of T if $Tv = av$ for some $\alpha \in F$. The element $a \in F$ is called an *eigenvalue* of T.

2.10. Remark. A linear transformation T has no fixed point if and only if 1 is not an eigenvalue of T. In accordance with Definition 1.9 a group of linear transformations Φ is fixed point free if and only if no element T in $\Phi \setminus \{I\}$ has 1 as eigenvalue.

2. Rational Canonical Form

We need some canonical form for linear transformations, so that we can handle the fixed point free automorphisms on elementary abelian groups. The rational canonical form has proven to be useful, and for a better understanding we develop it in general, following the outline of [**AW92**].

Let V be a vector space over a field F and let $T \in \mathrm{End}_F(V)$ be a fixed linear transformation.

$\mathrm{End}_F(V)$ is a ring using composition of linear transformations as multiplication. Define a function $\phi : F[x] \to \mathrm{End}_F(V)$ by sending x to T and $a \in F$ to $a * I$. Thus, if

$$f = a_0 + a_1 x + \ldots + a_n x^n,$$

then

$$\phi(f) = a_0 I + a_1 T + \ldots + a_n T^n.$$

ϕ is a ring homorphism. We will denote $\phi(f)$ by the symbol $f(T)$ and $\mathrm{Im}(\phi) = F[T]$. That is, $F[T]$ is the subring of $\mathrm{End}_F(V)$ consisting of polynomials in T. Then V is an $F[T]$ module by means of the multiplication

$$f(T)v = f(T)(v).$$

Using the homomorphism $\phi : F[x] \to F[T]$, we see that V is an $F[x]$ module with the scalar multiplication

$$fv = f(T)(v).$$

Let V_T denote V with the $F[x]$-module structure determined by T.

2.11. Proposition. Let V be a vector space over the field F of dimension $n < \infty$. If $T \in \mathrm{End}_F(V)$, then the R-module ($R = F[x]$) V_T is a finitely generated torsion R-module.

Proof. see [**AW92**], p. 234. □

2.12. Theorem. Let M be a non trivial finitely generated module over the principal ideal domain R. If the rank of M is n, then M is isomorphic to a direct sum of cyclic submodules

$$M \cong Rv_1 \oplus \cdots \oplus Rv_n$$

such that

$$R \neq \mathrm{Ann}(v_1) \supseteq \mathrm{Ann}(v_2) \supseteq \cdots \supseteq \mathrm{Ann}(v_n) = \mathrm{Ann}(M).$$

Proof. see [**AW92**], p. 156. □

According to Theorem 2.12, the R-module V_T can be written as a direct sum of cyclic R-submodules

$$V_T \cong Rv_1 \oplus \cdots \oplus Rv_k$$

such that $\mathrm{Ann}(v_i) = \langle f_i \rangle, f_i \in F[x]$ for $1 \leq i \leq k, f_i$ monic, and

$$f_i | f_{i+1} \text{ for } 1 \leq i \leq k.$$

The polynomials $f_1, \ldots, f_k$ are uniquely determined.

2.13. Definition ([AW92](4.4.6)).

(a) The monic polynomials $f_1, \dots, f_k$ above are called the *invariant factors* of the linear transformation T.
(b) The invariant factor f_k of T is called the *minimal polynomial* m_T of T.
(c) The *characteristic polynomial* c_T of T is the product of all the invariant factors of T, i.e., $c_T = f_1 f_2 \cdots f_k$.

2.14. Corollary. m_T is the unique monic polynomial of lowest degree such with

$$m_T(T) = 0.$$

PROOF. see [**AW92**], p. 235. □

There is another decomposition of a torsion R-module M into a direct sum of cyclic submodules which takes advantage of the prime factorization of any generator of $\operatorname{Ann}(M)$. To describe this decomposition we need the following definition.

2.15. Definition. Let M be a module over the principal ideal domain R and let $p \in R$ be a prime, i.e., if $p|ab$ implies that $p|a$ or $p|b$ for $a, b \in R$. Define the *p-component* M_p of M by

$$M_p = \{x \in M : \operatorname{Ann}(x) = \langle p^n \rangle \text{ for some natural number } n\}$$

If $M = M_p$, then M is said to be *p-primary*, and M is *primary* if it is p-primary for some prime $p \in R$.

2.16. Theorem. Any finitely generated torsion module M over a principal ideal domain R is a direct sum of primary cyclic submodules.

PROOF. see [**AW92**], p. 163. □

According to Theorem 2.16 V_T, can be further decomposed as a direct sum of primary cyclic R-submodules. Let $h_1, \dots, h_l$ be the set of distinct irreducible polynomials that occur as a divisor of some invariant factor of T. Then

$$\begin{aligned} f_1 &= h_1^{e_{11}} \cdots h_l^{e_{1l}} \\ &\vdots \\ f_k &= h_1^{e_{k1}} \cdots h_l^{e_{kl}} \end{aligned}$$

where the divisibility conditions imply that

$$0 \le e_{1j} \le e_{2j} \le \cdots \le e_{kj} \text{ for } 1 \le j \le l.$$

Let $V_i = Rv_i$ with $\operatorname{Ann}(v_i) = \langle f_i \rangle$ for $1 \le i \le k$ as above. Then

$$V_i \cong Rw_{i1} \oplus \cdots \oplus Rw_{il}$$

such that $\operatorname{Ann}(w_{ij}) = \langle h_j^{e_{ij}} \rangle$ for $1 \le j \le l$.

2.17. Definition. The polynomials $\{h_j^{e_{ij}} : e_{ij} > 0, 1 \le j \le l\}$ are called the *elementary divisors* of T.

There is a connection between polynomials and matrices, which we are going to use extensively.

2.18. Definition. Let $f = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \in F[x]$ be a monic polynomial. Then the *companion matrix* $C(f) \in M_n(F)$ of f is the $n \times n$ matrix

$$C(f) = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & 0 & -a_2 \\ \cdot & \cdot & & \cdot & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & 1 & 0 & -a_{n-2} \\ 0 & 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

We introduce the notation of partitioned matrices: suppose that A is an $m \times n$ matrix over F. If $m = \sum_{i=1}^{r}$ and $n = \sum_{j=1}^{s}$, then we may think of A as an $r \times s$ block matrix

$$A = \begin{pmatrix} A_{11} & \cdots & A_{1s} \\ \vdots & \ddots & \vdots \\ A_{r1} & \cdots & A_{rs} \end{pmatrix}$$

where each block A_{ij} is a matrix of size $m_i \times n_j$ with entries in F. If $r = s$ and if $A_{ij} = 0$ whenever $i \neq j$, then we call A a *block diagonal matrix* and denote A by

$$A = A_{11} \oplus \cdots \oplus A_{rr} = \bigoplus_{i=1}^{r} A_{ii}.$$

All these preliminaries now enable us to give a canonical form for every linear transformation.

2.19. Theorem (Rational canonical form, variant [AW92](4.4.17)). Let V be a vector space of dimension n over a field F and let $T \in \mathrm{End}_F(V)$ be a linear transformation. If $E = \{h_j^{e_{ij}} : e_{ij} > 0, 1 \leq j \leq l\}$ is the set of elementary divisors of the $F[x]$-module V_T, then V has a basis $\mathcal{B}$ such that

$$[T]_{\mathcal{B}} = \bigoplus_{g \in E} C(g).$$

Proof. Let

$$V_T \cong \bigoplus_{i=1}^{k} (Rw_{i1} \oplus \cdots \oplus Rw_{il}),$$

where $R = F[x]$ and $\mathrm{Ann}(w_{il}) = \langle h_j^{e_{ij}} \rangle$ with the stipulation that if $e_{ij} = 0$, then $Rw_{ij} = R0$, the trivial subspace of dimension 0 of V.

Suppose $e_{ij} > 0$. Let $\deg(h_j^{e_{ij}}) = n_{ij}$. Then

$$\mathcal{B}_{ij} = \{w_{ij}, T(w_{ij}), \ldots, T^{n_{ij}-1}(w_{ij})\}$$

is a set of n_{ij} linearly independent vectors, thus a basis for the cyclic submodule Rw_{ij}. Since submodules of V_T are precisely the T-invariant subspaces of V, it follows that $T|_{Rw_{ij}} \in \mathrm{End}_F(Rw_{ij})$ and

$$[T|_{Rw_{ij}}]_{\mathcal{B}_{ij}} = C(h_j^{e_{ij}}).$$

Since $\sum_{i,j:e_{ij}>0} n_{ij} = n$ and $\mathcal{B} = \bigcup_{i,j:e_{ij}>0} B_{ij}$ is a basis of V, we find

$$[T]_{\mathcal{B}} = \bigoplus_{i,j:e_{ij}>0} C(h_j^{e_{ij}})$$

and the theorem is proven. □

2.20. Corollary ([AW92](4.4.34)). Let V be a finite-dimensional vector space over a field F and let $T : V \to V$ be a linear transformation such that $T^k = I$. Suppose that F is a field in which the equation $z^k = 1$ has k distinct solutions. Then T is diagonalizable, i.e., there V has a basis $\mathcal{B}$ such that $[T]_{\mathcal{B}}$ is a diagonal matrix.

Proof. This is an equivalent formulation of Theorem 2.19 for the case of m_T being a product of distinct linear factors. □

We like to take a closer look on irreducible polynomials and finite fields now.

3. Polynomials over Finite Fields

2.21. Definition. Let $f \in F[x]$ be irreducible of degree greater than 0. Then the smallest natural number k with the property that $f|(x^k - 1)$ is called the *order* of the polynomial f.

2.22. Theorem. If f is an irreducible polynomial in $F_p[x]$ of degree e, then f has a root α in the extension field F_{p^e} of F_p. Furthermore, all the roots are simple and are given by the e distinct elements $\alpha, \alpha^p, \alpha^{p^2}, \dots, \alpha^{p^{e-1}}$ of F_{p^e}.

Proof. see [**LN84**], p. 52. □

2.23. Lemma. Let $f \in F_p[x]$ be an irreducible polynomial of order k and degree e. Then $k|p^e - 1$ and $k \nmid p^m - 1$ for $m < e$.

Proof. Since f has degree e, all its roots can be found within F_{p^e} by the theorem above. Thus $f|x^{p^e} - 1$ and by definition, the order k is a divisor of $p^e - 1$.

Suppose the e roots $\alpha, \alpha^p, \alpha^{p^2}, \dots, \alpha^{p^{e-1}}$ of f are elements of F_p^m for $m < e$. Then $\alpha^{p^m} = 1$ and $f(1) = 0$, which implies a contradiction to f being irreducible. □

CHAPTER 3

Structure of Fixed Point Free Automorphism Groups

The structure of fixed point free automorphism groups was determined by Zassenhaus in [**Zas36**] and [**Zas85**]. We basically follow the development of Robinson in [**Rob96**] and cite results from [**HB82**] and [**Wäh87**].

We serve the relations between a group G and a fixed point free automorphism group Φ on G as a starter.

1. Necessary Conditions on G and Φ

3.1. Proposition. Let Φ be a fixed point free automorphism group on a group G. Then $|\Phi|$ divides $|G|-1$.

PROOF. Since all automorphisms of Φ are fixed point free, the orbit of each $x \in G, x \neq 1_G$, under Φ is of size $|\Phi|$. Thus $G \setminus \{1_G\}$ has a partition into sets of size $|\Phi|$ and $|\Phi|$ is a divisor of $|G|-1$. □

3.2. Lemma ([Rob96](10.5.1)). Let α be a fixed point free automorphism of order n on the group G.

(a) If $\gcd(i,n)=1$, then α^i is also fixed point free.
(b) The mapping μ with $\mu : g \mapsto g^{-1}\alpha(g)$ is a permutation of G.
(c) g and $\alpha(g)$ are conjugate if and only if $g = 1_G$.
(d) $g\alpha(g)\alpha^2(g)\cdots\alpha^{n-1}(g) = 1_G$ for all $g \in G$.
(e) If $n = 2$, then $\alpha(g) = g^{-1}$ for all $g \in G$ and G is abelian.

PROOF.

(a) Any fixed point of α^i would also be a fixed point for α because α is a power of α^i.
(b) Suppose there are $g, h \in G$ such that $g^{-1}\alpha(g) = h^{-1}\alpha(h)$, then $\alpha(gh^{-1}) = gh^{-1}$ and $g = h$. Since G is finite, μ is a permutation.
(c) Suppose $\alpha(g) = g^x$ for some $g, x \in G$. By (b) there is some $y \in G$ such that $x = y^{-1}\alpha(y)$. Thus
$$\alpha(g) = g^x = \alpha(y)^{-1}ygy^{-1}\alpha(y)$$
and
$$\alpha(ygy^{-1}) = ygy^{-1}.$$
Therefore $ygy^{-1} = 1_G$ and $g = 1_G$.
(d) Let $h = g\alpha(g)\alpha^2(g)\cdots\alpha^{n-1}(g)$. Since $\alpha^n = \mathrm{id}_G$, we have
$$\alpha(h) = \alpha(g)\alpha^2(g)\cdots\alpha^{n-1}(g)g = g^{-1}hg$$
and $h = 1_G$ by (c).

(e) According to (b), every $g \in G$ has a unique representation $h^{-1}\alpha(h)$ for some $h \in G$ and

$$\alpha(g) = \alpha(h^{-1}\alpha(h)) = \alpha(h)^{-1}h = g^{-1}.$$

Thus $\alpha(g) = g^{-1}$ for all $g \in G$ and G has to be abelian since

$$g_2^{-1}g_1^{-1} = \alpha(g_1g_2) = \alpha(g_1)\alpha(g_2) = g_1^{-1}g_2^{-1}$$

for all $g_1, g_2 \in G$.

□

3.3. Proposition. Let G be a finite group with fixed point free automorphism group Φ.

(a) For each Φ-invariant non trivial subgroup $U < G$, the restriction $\Phi|_U$ is isomorphic to Φ.

(b) For $G = G_1 \times G_2$, a direct product, Φ_i fixed point free on $G_i, i = 1, 2$, and $a : \Phi_1 \mapsto \Phi_2$, an isomorphism, $\Phi := \{(\varphi, a(\varphi)) : \varphi \in \Phi_1\}$ operates on G without non trivial fixed points.

(c) (**[Hup67]** (V. 8.10)) For each Φ-invariant proper normal subgroup $N \lhd G$, the canonical $\bar{\Phi}$ acts on the factor group G/N as fixed point free automorphism group and is isomorphic to Φ.

Proof.

(a) Let $\Phi_U := \Phi|_U$ and suppose Φ_U is not isomorphic to Φ. As Φ_U is a homomorphic image of Φ, there has to be some $\mathrm{id}_G \neq \varphi \in \Phi$ that acts as identity mapping on U, i.e., all elements of U are fixed points of φ which is a contradiction to Φ being fixed point free on the whole group G.

(b) Suppose there is some $\varphi \in \Phi$ and $(g_1, g_2) \in G_1 \times G_2$ such that $\varphi(g_1) = g_1$ and $a(\varphi)(g_2) = g_2$. Either $\varphi = \mathrm{id}_{G_1}$ and $a(\varphi) = \mathrm{id}_{G_2}$, thus $(\varphi, a(\varphi))$ is the identity mapping on $G_1 \times G_2$ or (g_1, g_2) is the identity of $G_1 \times G_2$.

(c) Suppose there is

$$\bar{\varphi}(gN) = \varphi(g)N = gN$$

for some $g \in G, \varphi \in \Phi$. Then $g^{-1}\varphi(g) \in N$ and since φ is fixed point free on N, Proposition 3.2 gives $n \in N$ such that

$$g^{-1}\varphi(g) = n^{-1}\varphi(n).$$

Now $\varphi(gn^{-1}) = gn^{-1}$ and either $\varphi = \mathrm{id}_G$ or $g = n$. Thus $\bar{\Phi}$ is both isomorphic to Φ and fixed point free on G/N.

□

While some kind of converse for Proposition 3.3 can be used to derive all fixed point free automorphism groups on an abelian group G from fixed point free automorphism groups on elementary abelian factor groups of G, as we will see later on, the existence of isomorphic fixed point free automorphism groups on all invariant normal subgroups and factors generally does not imply the existence of a fixed point free automorphism group on the whole group in the non abelian case.

The smallest examples for this fact are the 2 non abelian groups G_1, G_2 of order 27. All nontrivial subgroups and factor groups are abelian of order 3 or 9 and therefore admit a fixed point free automorphism group of order 2 with the one fixed point free automorphism $i : x \mapsto x^{-1}$ (see Proposition 3.3 (a), (c)). But by Lemma 3.2 (e) there is a fixed point free automorphism of order 2 on a group if and only if the group is abelian. Therefore there is no fixed point free automorphism group on G_1 or G_2 at all.

3.4. Lemma ([Rob96](10.5.2)). If α is a fixed point free automorphism on a finite group G, then for each prime p there is a p-Sylow subgroup P such that $\alpha(P) = P$.

Proof. Let P_0 be any p-Sylow subgroup. Then $\alpha(P_0) = P_0^g$ for some $g \in G$ since all p-Sylow subgroups are conjugate. Applying Proposition 3.2 (b), we write $g = h^{-1}\alpha(h)$ for the suitable h. Let $P = P_0^{h^{-1}}$. Then

$$\alpha(P) = \alpha(hP_0h^{-1}) = hg\alpha(P_0)g^{-1}h^{-1} = P_0^{h^{-1}} = P$$

and the assertion is true for P. □

3.5. Lemma. Let H be a group of automorphisms of a finite abelian group A. Suppose that H is the semidirect product $\langle\sigma\rangle \ltimes M$ where $\sigma\beta$ is fixed point free of prime order p for every $\beta \in M$. Then $M = \langle \mathrm{id}_A \rangle$.

Proof. see [**Rob96**], p.305. □

The following theorem by Thompson is fundamental for our future development.

3.6. Theorem (Thompson). Let Φ be a fixed point free automorphism group on a group G. Then G is nilpotent.

Proof. see [**Rob96**], p.306.

Sketch: It suffices to show that G has to be nilpotent if it admits a fixed point free automorphism α of prime order p. Assume that the theorem is false and let G be a counter example of minimal order. By Proposition 3.3 (c) we see that $\bar{\alpha}$ is fixed point free on $G/C(G)$ and thus $C(G)$ is trivial for the reason that G is minimal. First we deal with the case where G is solvable, then the non solvable case is reduced with Thompson's criterion for p-nilpotence.

Let A be a minimal non trivial normal subgroup of G which is invariant under α. We conclude that A is an elementary abelian q-group for some prime q. By Lemma 3.4 there is an α-invariant r-Sylow subgroup of G for a prime r distinct from p and q.

If $AR \neq G$ for all $r \neq q$, then the minimality of $|G|$ forces AR to be nilpotent and $R \leq C_G(A)$ implying the contradiction that q divides $|C(G)|$. Thus $G = AR$ and after checking the presumptions, Lemma 3.5 can be applied on A with $\sigma = \alpha|_A$ and M the group of automorphisms of A that arise from conjugation by elements of R. This gives the contradiction $A \leq C(G)$.

For G non solvable there is an α-invariant q-Sylow subgroup Q for an odd prime divisor q of $|G|$. Since $|G|$ is minimal, all proper normal α-invariant subgroups are nilpotent. Thompson's criterion (see [**Rob96**], p.298) may be applied and shows that G is q-nilpotent. This leads to G being solvable. □

3.7. Theorem (Burnside). Let Φ be a fixed point free automorphism group on a group G.

(a) If the order of Φ is $|\Phi| = pq$ for p, q not necessarily distinct primes, then Φ is cyclic.

(b) The p-Sylow subgroups of Φ are cyclic for $p > 2$, they are cyclic or quaternion groups for $p = 2$.

Proof.

(a) Suppose Φ of order pq is not cyclic. Then some straightforward application of the Sylow Theorems 1.13 shows that $\Phi = \langle \alpha, \beta \rangle$ is a semidirect product where $\operatorname{ord} \alpha = p, \operatorname{ord} \beta = q$ such that $\langle \beta \rangle$ is normal. The element $\alpha\beta^i$ has order p for $0 \leq i \leq q-1$. Since G is nilpotent by Theorem 3.6, the center $C(G)$ is non trivial and Φ acts on it without fixed points, In particular, pq divides $|C(G)| - 1$. Thus we may apply Lemma 3.5 to Φ acting on $C(G)$, obtaining the contradiction that Φ is cyclic.

(b) All subgroups of order p^2 of Φ are cyclic by (a), implying that each p-Sylow subgroup of Φ has exactly one subgroup of order p. Theorem 1.25 identifies the p-groups with this property as cyclic or quaternion groups.

□

In the light of G being nilpotent if there is a fixed point free automorphism group Φ on G, we formulate the following:

3.8. Proposition. Let $G = \oplus_{i=1}^{m} G_i$ be the direct product of its p_i-Sylow subgroups G_i with $p_i, i = 1, \ldots m$, prime and let Φ be a fixed point free automorphism group on G. Then for all $i = 1, \ldots, m$ the restriction $\Phi|_{G_i}$ is fixed point free on G_i and isomorphic to Φ.

Proof. See Proposition 3.3 (a) and 1.15. □

2. Characterization of Φ

So groups where all p-Sylow subgroups are cyclic and groups with quaternion 2-Sylow subgroup and cyclic p-Sylow subgroups for all other primes are of particular interest in this context. Zassenhaus characterized all solvable groups with the above properties in [**Zas36**]. To be precise, he demanded that the 2-Sylow subgroups should have a cyclic subgroup of index 2. This requirement is certainly fulfilled in case of quaternion groups so that the solvable fixed point free automorphism groups occur as subclass of these groups.

We use a different approach, aiming directly at solvable groups Φ, which are described by Theorem 3.7 (b) and building them up by extension.

3.9. Lemma (Zassenhaus [Hup67](IV. 2.10)). If Φ'/Φ'' and Φ''/Φ''' are cyclic for a group Φ, then $\Phi'' = \Phi'''$.

Proof. By transition from Φ to Φ/Φ''' we can assume that Φ''' is trivial. Then we have to show, that Φ'' is also trivial.

Φ'' is cyclic and $N_\Phi(\Phi'')/C_\Phi(\Phi'')$ being isomorphic to a subgroup of $\operatorname{Aut}(\Phi'')$ has therefore to be abelian by Proposition 1.8. Thus $\Phi' \leq C_\Phi(\Phi'')$ and Φ'' is a subgroup of the center of Φ'. Since Φ'/Φ'' is cyclic, we have $\Phi' = \langle a, \Phi'' \rangle$ for some $a \in \Phi'$ and Φ' is abelian. Hence Φ'' is trivial. □

3.10. Lemma ([Hup67](IV. 2.9)). A finite group Φ, with all p-Sylow subgroups being cyclic, is solvable.

Proof. We use induction on the number of distinct prime divisors of $|\Phi|$. If Φ has prime power order, then the assertion is obvious. Now suppose the hypothesis holds for all groups for which the order is divisible by exactly n distinct primes.

Let p be the smallest of $n+1$ distinct prime divisor of $|\Phi|$ and let P be a p-Sylow subgroup of order p^d. Since $N_\Phi(P)/C_\Phi(P)$ can be embedded into $\operatorname{Aut}(P)$ which is a group of order $p^{d-1}(p-1)$ by Proposition 1.17, we find

$$N_\Phi(P) = C_\Phi(P).$$

Theorem 1.34 provides a normal subgroup N of Φ such that

$$\Phi/N \cong P.$$

While N is solvable by assumption, Φ/N is solvable as a cyclic group. Eventually, Φ is solvable. □

The next theorem, due to Zassenhaus, describes the structure of any group, where all p-Sylow subgroups are cyclic.

3.11. Theorem ([Hup67](IV. 2.11)). Let all p-Sylow subgroups of a group Φ be cyclic. Then Φ is generated by elements a and b fulfilling the following relations:

$$a^m = b^n = \mathrm{id}, b^{-1}ab = a^r, \tag{I}$$

where $r^n \equiv 1 \bmod m, m$ is odd, $0 \leq r < m, \gcd(m, n(r-1)) = 1$ and $|\Phi| = mn$. The derived subgroup $\Phi' = \langle a\rangle$ and the factor group $\Phi/\Phi' = \langle b \cdot \Phi'\rangle$ are cyclic, $|\Phi'| = m$ and $|\Phi/\Phi'| = n$. Every group fulfilling the above relations has only cyclic p-Sylow subgroups.

Proof. Since the abelian groups Φ'/Φ'' and Φ''/Φ''' have only cyclic Sylow subgroups, both Φ'/Φ'' and Φ''/Φ''' are cyclic. Lemma 3.9 implies that $\Phi'' = \Phi'''$ and since Φ is solvable by Lemma 3.10, Φ'' is trivial.

Let $\Phi' = \langle a\rangle$ and $\Phi/\Phi' = \langle b\cdot\Phi'\rangle$ for some $a, b \in \Phi$, let $\operatorname{ord} a = m$ and $\operatorname{ord} b\cdot\Phi' = n$. Then $b^n = a^s \in \langle a\rangle$ and $b^{-1}ab = a^r \in \langle a\rangle$ for integers r, s. Since

$$a^{r^n} = b^{-n}ab^n = a^{-s}aa^s = a,$$

we have $r^n \equiv 1(m)$.

Let $x = b^ia^j, y = b^ua^v$ be two arbitrary elements of Φ:

$$\begin{aligned}[x,y] &= (a^{-j}b^{-i})(a^{-v}b^{-u})(b^ia^j)(b^ua^v)\\ &= a^{-j}(b^{-i}a^{-v}b^i)(b^{-u}a^jb^u)a^v\\ &= a^{-j}a^{-vr^i}a^{jr^u}a^v\\ &= a^{j(r^u-1)-v(r^i-1)}\end{aligned}$$

and $[x,y]$ is a power of the commutator $[a,b] = a^{r-1}$. Thus a^{r-1} generates $\Phi' = \langle a\rangle$ and $\gcd(m, r-1) = 1$. Now

$$a^s = b^n = b^{-1}b^nb = b^{-1}a^sb = a^{rs}$$

implies $s(r-1) \equiv 0 \bmod m$ and $s \equiv 0 \bmod m$, i.e., $\operatorname{ord} b = n$.

If a prime p were to divide both m and n, then $\langle a^{m/p}, b^{n/p}\rangle$ would be a non cyclic subgroup of order p^2, contradicting the hypothesis. Thus $\gcd(m,n) = 1$.

Conversely, assume that Φ has the presentation given above and let P be a p-Sylow subgroup. Then Φ has order mn and either $P \leq \langle a\rangle$ or a conjugate of P is in $\langle b\rangle$ since $\gcd(m,n) = 1$. In either case, P is cyclic. □

We will refer to the groups described in the above Theorem 3.11 as groups of type (I) in accordance with [**Wol67**] and [**Wäh87**] as they represent our first class of groups fulfilling the properties given in Theorem 3.7 (b). Cyclic groups are represented in this form as $\langle b\rangle$ with a being the identity. We mention that groups which have a cyclic normal subgroup with cyclic factor group are called *metacyclic* in [**Hup67**] and [**Rob96**] without making further use of this name.

Note that having type (I) alone does not qualify a group to be isomorphic to a fixed point free automorphism group. For instance the symmetric group on 3 points, S_3, has order 6 and all p-Sylow subgroups are cyclic. S_3 can be represented as in Theorem 3.11 but a fixed point free automorphism group with order a product of two primes has to be cyclic by Theorem 3.7 (a). We will refine our characterization by requiring an additional condition forcing every subgroup of Φ of order pq to be cyclic later on.

Next we are going to investigate those groups with quaternion 2-Sylow subgroups and cyclic p-Sylow subgroups for $p > 2$. The results of the following Theorems 3.12 to 3.16 were basically found by Zassenhaus in [**Zas36**]. The formulations and proofs given here are new.

3.12. Theorem. Let Φ be a group with quaternion 2-Sylow subgroups and cyclic p-Sylow subgroups for $p > 2$. If the derived subgroup Φ' has a cyclic 2-Sylow subgroup, then Φ' is cyclic and Φ is generated by elements a, b, q fulfilling the following relations:

$$\text{(II)} \qquad a^m = b^n = \mathrm{id}, b^{-1}ab = a^r, q^2 = b^{n/2}, q^{-1}aq = a^k, q^{-1}bq = b^l,$$

where $n = 2^t u, t > 1, u$ odd, $2^t | l + 1$ and $n | l^2 - 1$ as well as $r^{2u} \equiv r^{l-1} \equiv k^2 \equiv 1(m), \gcd(m, n(r-1)) = 1$. The order of Φ is $|\Phi| = 2mn$ and $H = \langle a, b\rangle$ is a subgroup of type (I) and index 2.

Proof. Since Φ' has cyclic p-Sylow subgroups for all primes p, we have that Φ'/Φ'' and Φ''/Φ''' are cyclic and Lemma 3.9 applies to $\Phi'' = \Phi''' = \langle \mathrm{id}\rangle$. Thus Φ' has to be abelian and even cyclic.

Let $Q = \langle p, q\rangle$ with $p^{2^t} = \mathrm{id}, q^2 = p^{2^{t-1}}, q^{-1}pq = p^{-1}$ be a quaternion 2-Sylow subgroup of Φ of order 2^{t+1}. Since $Q' = \langle p^2\rangle \leq \Phi'$ there is a 2-Sylow subgroup Q^* of Φ' including Q'. According to the assumption Q^* is cyclic and thus either $Q^* = \langle p^2\rangle$ or $Q^* = \langle p\rangle$.

Suppose $Q^* = \langle p^2\rangle$. The abelian factor group Φ/Φ' has a 2-Sylow subgroup isomorphic to Z_2^2 and cyclic p-Sylow subgroups for $p > 2$ because Φ has some. Then

$$\Phi/\Phi' \cong Z_2 \times Z_2 \times Z_n$$

where $2 \nmid n$, i.e., $\exists v \in \Phi$ such that $v^n \in \Phi'$ and $\Phi/\Phi' = \langle p \cdot \Phi', q \cdot \Phi', v \cdot \Phi'\rangle$

The group $H := \langle p, v, \Phi'\rangle$ is of order $|\Phi|/2$ and has only cyclic p-Sylow subgroups.

Suppose $Q^* = \langle p\rangle$. Then

$$\Phi/\Phi' \cong Z_2 \times Z_n$$

where $2 \nmid n$, i.e., $\exists v \in \Phi$ such that $v^n \in \Phi'$ and $\Phi/\Phi' = \langle q \cdot \Phi', v \cdot \Phi'\rangle$.

The group $H := \langle v, \Phi'\rangle$ is of order $|\Phi|/2$ and has only cyclic p-Sylow subgroups.

In both cases H is a subgroup of Φ of index 2, that is, H is normal, and has a representation $H = \langle a, b\rangle$ as given by Proposition 3.11. The divisibility conditions on $\operatorname{ord} a$ and $\operatorname{ord} b$ imply that $\operatorname{ord} a = m$ is odd. Thus we have $\operatorname{ord} b = n = 2^t u$ with $2 \nmid u$ and $b^u = p$, w.l.o.g.

Since $H' = \langle a\rangle$ is characteristic in Φ' and therefore normal in Φ, it holds $q^{-1}aq = a^k$ where $\gcd(m, k) = 1$. The element $q^2 = p^{2^{t-1}} \in \Phi'$ commutes with

$a \in \Phi'$ since Φ' is cyclic. So

$$a = q^{-2}aq^2 = a^{k^2}$$

and $k^2 \equiv 1 \bmod m$.

There are exactly m distinct subgroups of order n in H, namely the groups of the form $\langle ba^i \rangle$ for $0 \leq i \leq m-1$. The orbits of these groups under conjugation by q have a power of 2 as length and since m is odd, there has to be one subgroup of order n which is fixed by q, w.l.o.g., $q^{-1}bq = b^l$ for some integer l. Then,

$$b = q^{-2}bq^2 = q^{-1}b^lq = b^{l^2}$$

and $l^2 \equiv 1 \bmod n$. Furthermore,

$$b^{-u} = q^{-1}b^uq = (b^l)^u = b^{lu}$$

and $l \equiv -1 \bmod 2^t$. Since the commutator

$$[b^u, q] = b^{-u}q^{-1}b^uq = b^{-2u}$$

is an element of Φ' and $a \in \Phi'$, it holds that b^{2u} commutes with a because Φ' is cyclic. Hence,

$$a = b^{-2u}ab^{2u} = a^{r^{2u}}$$

and $r^{2u} \equiv 1 \bmod m$. Similarly, for $b^{-1}q^{-1}bq = b^{l-1}$ we have $r^{l-1} \equiv 1 \bmod m$. □

The following two Lemmata prove to be useful.

3.13. Lemma. Let Φ be a group with quaternion 2-Sylow subgroups and cyclic p-Sylow subgroups for $p > 2$.

(a) If Φ' has a quaternion 2-Sylow subgroup, then Φ/Φ' is cyclic and $4 \nmid [\Phi : \Phi']$.
(b) If Φ'' has a quaternion 2-Sylow subgroup, then Φ/Φ'' has type (I) and $2 \nmid [\Phi' : \Phi'']$.
(c) If Φ''' has a quaternion 2-Sylow subgroup, then $\Phi''' = \Phi''$.

Proof.

(a) Let $Q = \langle p, q \rangle$ with $p^{2^t} = \mathrm{id}, q^2 = p^{2^{t-1}}, q^{-1}pq = p^{-1}$ be a quaternion 2-Sylow subgroup of order 2^{t+1} of Φ. Since $Q' = \langle p^2 \rangle \leq \Phi'$, there is a 2-Sylow subgroup Q^* of Φ' including Q'. According to the assumption Q^* is quaternion and thus either $Q^* = \langle p^2, q \rangle$ or $Q^* = \langle p, q \rangle = Q$.

Suppose $Q^* = \langle p^2, q \rangle$. The abelian factor group Φ/Φ' has a 2-Sylow subgroup $\langle p \cdot \Phi' \rangle$ of order 2 and cyclic s-Sylow subgroups for primes $s > 2$ because Φ has. Thus Φ/Φ' is cyclic.

Suppose $Q^* = Q$. Then Φ/Φ' is of odd order and has only cyclic s-Sylow subgroups. This results again in Φ/Φ' being cyclic.

(b) Φ/Φ' and Φ'/Φ'' are cyclic according to (a) and there is a 2-Sylow subgroup Q^{**} of Φ'' either equal $Q = \langle p, q \rangle, \langle p^2, q \rangle$ or $\langle p^4, q \rangle$. In any case, Φ/Φ'' has only cyclic p-Sylow subgroups, i.e., is of type (I).

The derived subgroup of the factor group is

$$(\Phi/\Phi'')' = (\Phi' \cdot \Phi'')/\Phi'' = \Phi'/\Phi''.$$

According to Theorem 3.11 the orders $|\Phi/\Phi'|$ and $|\Phi'/\Phi''|$ are relatively prime and moreover, $|\Phi'/\Phi''|$ is odd.

(c) Since Φ'/Φ'' and Φ''/Φ''' are cyclic, Lemma 3.9 gives $\Phi'' = \Phi'''$.

□

3.14. Lemma. If Φ' has a quaternion 2-Sylow subgroup Q and Φ'' is cyclic, i.e., Φ' is of type (II), for a group Φ, then $\Phi' = \langle a \rangle \times Q$ with some a of odd order and $|Q| = 8$.

Proof. Let $Q = \langle p, q \rangle$ with $q^{-1}pq = p^{-1}$ be a quaternion 2-Sylow subgroup of Φ'.

$\Phi'' \lhd \Phi$ and by Proposition 1.8 the factor group $\Phi / C_\Phi(\Phi'')$ can be embedded into $\mathrm{Aut}(\Phi'')$ which is abelian since Φ'' is cyclic according to Theorem 3.12. This allows us to conclude that $\Phi' \le C_\Phi(\Phi'')$ and $\Phi'' \le C(\Phi')$. By Theorem 3.12 again there is a subgroup $H = \langle u, v \rangle$ of type (I) and index 2 in Φ'. Evidently, $H' = \langle u \rangle \le \Phi''$ and $H' \le C(\Phi')$ if and only if $u = \mathrm{id}$. Moreover, $[p, q] = p^{-2} \in \Phi''$ implies that $p^2 = q^2$ and $|Q| = 8$.

Thus $H = \langle v \rangle$ is cyclic of order $4n$ with n odd. We are free to assume $v^n = p \in Q$ and $q \in \Phi' \setminus H$.

Let $q^{-1}vq = v^l$ for some l such that $1 < l < 4n$. Then the commutator $[v, q] = v^{l-1} \in \Phi''$ has to commute with every element of Φ', in particular

$$v^{l-1}q = v^{-1}q^{-1}vqq = v^{-1}qv$$

and

$$qv^{l-1} = vqv^{-1}$$

have to coincide. We have used the fact that $q^2 = p^2$ as the unique element of order 2 in Φ'' is in the center of H.

$$\mathrm{id} = (v^{-1}qv)(vq^{-1}v^{-1}) = v^{-1}(q^{-1}v^2q)v^{-1} = v^{2l-2}$$

determines $l = 2n + 1$. Since $q^{-1}v^4q = v^{8n+4} = v^4$, we find that q commutes with every element of odd order in H and $\Phi' = \langle a \rangle \times \langle p, q \rangle$ where $a = v^4$. □

3.15. Theorem. Let Φ be a solvable group with a quaternion 2-Sylow subgroup Q and cyclic p-Sylow subgroups for $p > 2$. If Q has order 8 and $Q \le \Phi'$, then Φ is generated by elements a, b, p, q fulfilling the following relations:

$$\text{(III)} \qquad a^m = b^n = \mathrm{id}, b^{-1}ab = a^r, p^4 = \mathrm{id}, q^2 = p^2,$$
$$q^{-1}pq = p^{-1}, ap = pa, aq = qa, b^{-1}pb = q, b^{-1}qb = pq$$

where m, n are odd, $m | r^n - 1, 3 | n$ and $0 \le r < m, \gcd(m, n(r-1)) = 1$.

$H = \langle a, b \rangle$ is a group of type (I) and of odd order, $Q = \langle p, q \rangle \lhd \Phi$ and $\Phi = HQ$ is a semidirect product of H and Q. The derived subgroup $\Phi' = \langle a \rangle \times \langle p, q \rangle$ is of type (II) and $\Phi'' = \langle p^2 \rangle$.

Proof. Let Q be a quaternion 2-Sylow subgroup of Φ such that $Q \le \Phi'$ and let $N = N_\Phi(Q)$ denote the normalizer of Q in Φ. By Theorem 1.33 there is a subgroup H such that $N = HQ$ and $H \cap Q = \{\mathrm{id}\}$; of course, H has odd order. However, $H/C_H(Q)$ is isomorphic to a subgroup of $\mathrm{Aut}(Q)$ which is of order 24 by Proposition 1.26. Thus $[H : C_H(Q)]$ divides 3 and either $N = H \times Q$ or there is $b \in N_H(Q) \setminus C_H(Q)$ with $b^3 \in C_H(Q)$.

Applying Grün's First Theorem 1.35 we have

$$Q \cap \Phi' = \langle Q \cap N', Q \cap g^{-1}Q'g | g \in \Phi \rangle.$$

Now $N = H \times Q$ implies $Q \cap N' = Q \cap (H' \times Q') = \langle p^2 \rangle$ and since $Q \cap g^{-1}Q'g = Q \cap g^{-1}\langle p^2 \rangle g$ is a group of order 2 at most, we find that $Q \cap \Phi'$ is generated by elements of order 2. There is only one element of order 2 in Q, namely p^2 and $Q \cap \Phi' = \langle p^2 \rangle$, contrary to our assumption.

So we assume there is $b \in N_H(Q) \setminus C_H(Q)$ with $b^3 \in C_H(Q)$. By letting b operate on Q by conjugation we separate Q into orbits with sizes some power of 3. In particular, there is one element $p \in Q$ of order 4 with $b^{-1}pb \neq p$. If $b^{-1}pb$ were equal to p^{-1}, then $p = b^{-3}pb^3 = p^{-1}$. Thus b permutes the 3 cyclic subgroups of Q order 4 by conjugation without leaving any of them fixed;

$$b^{-1}pb = q$$

for some $q \notin \langle p \rangle$ and, w.l.o.g.,

$$b^{-1}qb = pq.$$

Each element of a quaternion group $Q_{2^{t+1}}$ is conjugate to its inverse within $Q_{2^{t+1}}$ as can be seen easily using the defining relations. With the additional equations $b^{-1}pb = q$ and $b^{-1}qb = pq$ all elements of order 4 of Q are conjugate in N by now. Moreover, the Sylow theorems imply all elements of order 4 in Φ are conjugate.

The relations above can be evaluated to

$$[p, b] = p^{-1}b^{-1}pb = p^{-1}q, [q, b] = q^{-1}b^{-1}qb = p^{-1}$$

and this allows us to conclude that $p, q \in N'$, thus $Q \leq N' \leq \Phi'$. We note that 3 to be divisor of $|\Phi|$ is not a sufficient but a necessary condition for Φ' to have a quaternion subgroup.

Suppose $Q \leq \Phi''$. Then some $b' \in \langle b \rangle$ with order a power of 3 and $b' \notin C_\Phi(Q)$ has to be in Φ'. Obviously, the factor group Φ/Φ'' has type (I) and odd order. The divisibility conditions on $|\Phi/\Phi'|$ and $|\Phi'/\Phi''|$ as given in Theorem 3.11 force $3 \nmid |\Phi'/\Phi''|$ if $|\Phi/\Phi'|$ is odd. Thus $b' \in \Phi''$ and again $Q \leq \Phi'''$. Both Φ'/Φ'' and Φ''/Φ''' are cyclic, resulting in $\Phi'' = \Phi'''$ by Lemma 3.9 in contradiction to Φ being solvable.

Hence Φ'' has cyclic 2 Sylow subgroups, Φ' is of type (II) and we can apply Lemma 3.14 to determine

$$\Phi' = \langle a \rangle \times Q$$

with some a of odd order and $|\Phi'''| = 2$. Moreover, $Q = \langle p, q \rangle$ is characteristic in Φ' and also in Φ. Thus, eventually, we have shown that

$$\Phi = N = HQ$$

the semidirect product of a group H of type (I) with odd order and a quaternion group Q of order 8.

$$H = \langle a, b \rangle$$

with $b \notin C_H(Q)$ having the properties described above. $a^m = b^n = \mathrm{id}, b^{-1}ab = a^r$ and $\gcd(m, n(r-1)) = 1, m|r^k - 1$ as in Theorem 3.11. □

Note that the implication given in [**Wäh87**] on page 21, namely that $T = \langle b^{n/3}, p, q \rangle \cong SL(2,3)$ is not true if $9|n$. It can be seen from the above proof that for this case $b^{n/3}$ would be in $C_\Phi(\langle p, q \rangle)$ and $T = \langle b^{n/3} \rangle \times \langle p, q \rangle$. Nonetheless, it can be shown that $\Phi/\langle b^3, a \rangle \cong SL(2,3)$.

3.16. Theorem. Let Φ be a solvable group with a quaternion 2-Sylow subgroup Q and cyclic p-Sylow subgroups for $p > 2$. If the order of Q is greater than 8 and Φ' has a quaternion 2-Sylow subgroup Q^*, then Φ is generated by elements a, b, p, q, z fulfilling the following relations:

$$\begin{aligned} &a^m = b^n = \mathrm{id}, b^{-1}ab = a^r, p^4 = \mathrm{id}, p^2 = q^2 = z^2, \\ \text{(IV)} \qquad &q^{-1}pq = p^{-1}, ap = pa, aq = qa, z^{-1}az = a^k, b^{-1}pb = q, \\ &b^{-1}qb = p^2q, z^{-1}bz = b^l, z^{-1}pz = qp, z^{-1}qz = q^{-1} \end{aligned}$$

where m, n are odd, $3|n, 0 \leq r < m, \gcd(m, n(r-1)) = 1$ and $r^n \equiv r^{l-1} \equiv k^2 \equiv 1 \bmod m, l \equiv 2 \bmod 3, l^2 \equiv 1 \bmod n$.

Φ has order $16mn$, $H = \langle a, b, p, q\rangle$ is a subgroup of Φ of type (III) and index 2.

Proof. We start similarly to the proof of Theorem 3.15, where we characterized the groups of type (III).

Let $N = N_\Phi(Q)$ denote the normalizer of $Q = \langle u, v\rangle$ in Φ. By Theorem 1.33 there is a subgroup H such that $N = HQ$ and $H \cap Q = \{\mathrm{id}\}$; of course, H has odd order. However, $H/C_H(Q)$ is isomorphic to a subgroup of $\mathrm{Aut}(Q)$ which is a 2-group for $|Q| \geq 16$ by Proposition 1.28. Thus $H = C_H(Q)$ and $N = H \times Q$.

By Grün's First Theorem 1.35 we have

$$Q \cap \Phi' = \langle Q \cap N', Q \cap x^{-1}Q'x : x \in \Phi\rangle.$$

Now $Q \cap N' = Q \cap (H' \times Q') = \langle u^2\rangle$ and $Q \cap \Phi'$ is a quaternion subgroup if and only if there is $x \in \Phi$ such that $\langle u^2, x^{-1}u^2x\rangle$ is a quaternion group. In particular u^2 has order 4, see Proposition 1.28. Setting $p = u^2$ and $q = v$ we can assume

$$\exists x \in \Phi \;\; x^{-1}px = q.$$

Then $\langle p, q\rangle$ will be a quaternion subgroup of Φ' of order 8. According to Lemma 3.13 we have to distinguish between the two possibilities that Φ' is of type (II) or Φ'' is of type (II).

Suppose Φ' is of type (II). Lemma 3.14 states $\Phi' = \langle a\rangle \times Q^*$ with some $a \in \Phi'$ of odd order and $|Q^*| = 8$. Moreover, Q^* is characteristic, i.e.,

$$Q^* = \langle p, q\rangle$$

actually equals the intersection of all 2-Sylow subgroups of Φ. Since the index $[\Phi : \Phi']$ is not divisible by 4, it follows that $|Q| = 16$.

The number of 2-Sylow subgroups of Φ is given by $[\Phi : N_\Phi(Q)]$, odd. Since Q' is characteristic in Q, we have $N_\Phi(Q) \leq N_\Phi(Q')$ and $[\Phi : N_\Phi(Q')]$ divides $[\Phi : N_\Phi(Q)]$. Thus the number of conjugates to $Q' = \langle p\rangle$ is odd and $\langle p\rangle, \langle q\rangle$ and $\langle pq\rangle$ are conjugate, i.e., all 6 elements of order 4 of Q^* are conjugate under Φ. There has to be an element $x \in \Phi \setminus C_\Phi(Q^*)$ such that

$$x^3 \in C_\Phi(Q^*)$$

and $x^{-1}px = q$. By the same arguments as given in the proof of 3.15 we find $x^{-1}qx = pq$.

$x \notin \Phi'$, otherwise Φ' would be of type (III). So 3 is a divisor of $[\Phi : \Phi']$ and since Φ/Φ' is cyclic, there is $w \in \Phi$ such that $w^{2n} \in \Phi'$, where n is odd and $3|n$ and $\Phi = \langle w, \Phi'\rangle$.

$H = \langle w^2, \Phi'\rangle$ has index 2 in Φ. Thus $x \in H$ and H is a group of type (III).

Suppose Φ'' is of type (II). By Lemma 3.14 the 2-Sylow subgroup of Φ'' has order 8 and by Lemma 3.13 we have $2 \nmid [\Phi' : \Phi'']$. Thus Φ' is of type (III) and there is $w \in \Phi$ such that $w^{2n} \in \Phi'$ where n is odd and $\Phi = \langle w, \Phi' \rangle$.

$H = \langle w^2, \Phi' \rangle$ has index 2 in Φ and evidently is of type (III).

In any case, H has a representation $\langle a, b, p, q \rangle$ with relations as given in Theorem 3.15 and

$$\Phi = \langle a, b, p, q, z \rangle$$

with some $z \in \Phi \setminus H$ and $z^2 \in H$. The 2-Sylow subgroups of Φ have order 16.

In order to end up with a nice presentation of Φ we choose $z \in \Phi \setminus H$ such that

$$z^{-1} \langle a, b \rangle z = \langle a, b \rangle$$

which is possible because all complements of Q^* in H are conjugate by Theorem 1.33. Since $b^{-1}pb = q$ implies $pbp^{-1} = bqp^{-1} \notin \langle a, b \rangle$, we see that p and in fact all other elements of order 4 in Q^* do not have this property. Consequently, z can not be of order 8, which would mean $z^2 = p$ for instance, but z has order 4 and

$$z^2 = p^2 = q^2.$$

Furthermore, z commutes neither with p, q nor pq, otherwise $z \in \langle p \rangle, \langle q \rangle$ or $\langle pq \rangle$, respectively.

$\langle a \rangle$ is a characteristic subgroup of Φ and therefore

$$z^{-1} a z = a^k$$

for some integer k. Since $a \in C_G(Q^*)$, we have

$$a = z^{-2} a z^2 = a^{k^2}$$

and for $m = \operatorname{ord} a$ it holds $m | k^2 - 1$. The length of orbits on the complements of $\langle a \rangle$ in $\langle a, b \rangle$ is given by powers of 2 and the number of complements is odd. At least one of them is fixed and since they all are conjugate by elements of $\langle a \rangle$, where a commutes with the elements of Q^*, we can assume

$$z^{-1} b z = b^l$$

for some integer l and $b^{-1}pb = q, b^{-1}qb = pq$.

The orbits on the 3 maximal subgroups of Q^* generated by p, q and pq respectively under conjugation by z have length 1 or 2. Thus one of them, w.l.o.g., $\langle q \rangle$, gets fixed and

$$z^{-1} q z = q^{-1}.$$

Now $z^{-1}pz \neq p^{-1}$ because otherwise $z^{-1}pqz = p^{-1}q^{-1} = pq$ means z and pq commute. Thus $z^{-1}pz = (pq)^i$ where $i = \pm 1$ because these are the only remaining elements of order 4 in Q^*. The conjugation of $b^{-1}pb = q$ by z implies $b^{-l}(pq)^i b^l = q^{-1}$. The relations

$$b^{-1}pb = q, b^{-2}pb^2 = pq, b^{-3}pb^3 = p$$

force us to conclude that $i = -1$,

$$z^{-1} p z = qp$$

and $l \equiv 2 \bmod 3$. We conjugate $a^r = b^{-1}ab$ by z to obtain

$$a^{rk} = b^{-l} a^k b^l = a^{kr^l}$$

and thus $m|r^{l-1}-1$. Since b and $z^2=p^2$ commute,

$$b=z^{-2}bz^2=b^{l^2},$$

implying $n|l^2-1$ for $n=\operatorname{ord}b$. □

We summarize the results found above in one statement characterizing all solvable finite fixed point free automorphism groups.

3.17. Theorem ([Wol67], 6.1.11). Φ is a finite solvable group, where every subgroup of order a product of two primes is cyclic, if and only if Φ is isomorphic to one of the following groups

Type	Generators	Relations	Conditions
I	a,b	$a^m=b^n=\mathrm{id}$, $b^{-1}ab=a^r$	$\gcd(m,n(r-1))=1$, $r^n\equiv 1 \bmod m$
II	a,b,q	as in I; also $b^{n/2}=q^2$, $q^{-1}aq=a^k$, $q^{-1}bq=b^l$	as in I; also $n=2^tu, t\geq 2, u$ odd, $l\equiv -1 \bmod 2^t$, $l^2\equiv -1 \bmod u$, $r^{l-1}\equiv k^2\equiv 1 \bmod m$
III	a,b,p,q	as in I; also $p^4=\mathrm{id}, p^2=q^2$, $q^{-1}pq=p^{-1}$, $ap=pa, aq=qa$, $b^{-1}pb=q, b^{-1}qb=pq$	as in I; also m,n odd, $n\equiv 0 \bmod 3$
IV	a,b,p,q,z	as in III; also $p^2=z^2, z^{-1}pz=qp$, $z^{-1}qz=q^{-1}$, $z^{-1}az=a^k, z^{-1}bz=b^k$	as in III; also $r^{l-1}\equiv k^2\equiv 1 \bmod m$, $l^2\equiv 1 \bmod n$, $l\equiv 2 \bmod 3$

with the additional condition that if d is the smallest natural number such that $r^d\equiv 1 \bmod m$, then n/d is divisible by any prime divisor of d.

Proof. Suppose every subgroup of the finite solvable group Φ with order st for some primes s,t is cyclic. The proof of Proposition 3.7 (b) shows that each p-Sylow subgroup of Φ for an odd prime p has to be cyclic and each 2-Sylow subgroup is either cyclic or quaternion. Thus Φ is isomorphic to one of the groups described in Theorem 3.11, 3.12, 3.15 and 3.16.

Let $H=\langle a,b\rangle \leq \Phi$ with a,b described as for the isomorphism type of Φ. Furthermore, let d be the smallest natural number such that $m|r^d-1$. Let $n=\operatorname{ord}b$ and let t be a prime divisor of d which does not divide n/d. Let s be a prime divisor of m. Then $\langle a^{m/s},b^{n/t}\rangle$ has order st and has to be cyclic. Therefore,

$$a^{\frac{m}{s}}=b^{-\frac{n}{t}}a^{\frac{m}{s}}b^{\frac{n}{t}}=a^{\frac{m}{s}r^{n/t}}$$

which means $\frac{m}{s}(r^{n/t}-1)\equiv 0 \bmod m$ which is the case if and only if

$$s|(r^{n/t}-1)$$

for all prime divisors s of m.

By definition, $d|n$ and since t is prime, either $\gcd(d,n/t)=d$ or $\gcd(d,n/t)=d/t$. The first case implies that t divides (n/d) in contradiction to our assumption.

Thus we are forced to conclude that $\gcd(d, n/t) = d/t$ and

$$s|(r^{d/t} - 1)$$

for all s. We evaluate

$$\begin{aligned} r^d - 1 &= (r^{d/t} - 1)\sum_{i=0}^{t-1} r^{id/t} \\ &\equiv (r^{d/t} - 1)\sum_{i=0}^{t-1} 1 \bmod s \\ &\equiv (r^{d/t} - 1)t \bmod s. \end{aligned}$$

Thus $m|(r^d - 1)$ actually implies that $m|(r^{d/t} - 1)$ since $\gcd(s, t) = 1$ for every prime divisor s of m. This contradicts the minimality of d. Hence, if a prime t divides d, it also divides n/d.

Conversely, suppose Φ is a group with one of the presentations (I) to (IV) and let n/d be divisible by any prime divisor of n. Since all s-Sylow subgroups of Φ are cyclic or quaternion groups, every group of order s^2 with s prime is cyclic. If 2 is a divisor of $|\Phi|$ where Φ is of the type (II),(III) or (IV), then there is a unique element i of order 2 in Φ, thus $i \in C(\Phi)$ and all groups of order $2s$ are abelian, even cyclic.

For a group U of order st for two distinct odd primes s and t or $t = 2$ in case of Φ having type (I), there exists a conjugate which lies in $H = \langle a, b\rangle$, where a and b are the elements of these names in the presentation of Φ. For proving that U is cyclic, we only have to deal with the case that $s|m$ and $t|n$ for $m = \operatorname{ord} a$ and $n = \operatorname{ord} b$. Otherwise, we could find a conjugate of U either in $\langle a\rangle$ or $\langle b\rangle$ and everything is clear. Thus we assume that U is conjugate with $\langle a^{m/s}, b^{n/t}\rangle$ and since $d|(n/t)$ implies $b^{n/t} \in \langle b^d\rangle$ and b^d commutes with a, we conclude that U is cyclic as the conjugate of a cyclic group. □

3.18. Corollary. Let Φ be a fixed point free automorphism group of square free order on the group G. Then Φ is cyclic.

Proof. Φ has type (I) and the additional condition that $p|(n/d)$ if $p|d$ from Theorem 3.17 implies $d = 1$. Thus $m|r - 1$, i.e., r=1, and Φ is cyclic. □

We lack a characterization of non solvable fixed point free automorphism groups which we add right now.

3.19. Theorem (Zassenhaus [Zas85]). If Φ is a non trivial fixed point free automorphism group of some finite group and $\Phi = \Phi'$, then $\Phi \cong \mathrm{SL}(2, 5)$.

Proof. For the proof which exceeds this thesis we refer to the article [**Zas85**] by Zassenhaus himself or to the presentation in [**HB82**], p.387-413.

The idea is to start with an investigation of the maximal proper subgroups H of Φ which are solvable, based on Theorem 3.17. The non solvable maximal subgroups of Φ are dealt with induction on $|\Phi|$. Then the maximal cyclic subgroups and their normalizers are determined to obtain a partition of Φ into conjugacy classes. The final step is done using character theory. □

3.20. Theorem (Zassenhaus [Zas85]). If Φ is a non solvable fixed point free automorphism group of some finite group, then Φ has a subgroup H of the form

$$H \cong \mathrm{SL}(2,5) \times U$$

such that $[\Phi : H] \leq 2$, and where U is of type (I) and $\gcd(|U|, 30) = 1$.

Proof. see [**Wäh87**], p.335. □

CHAPTER 4

The Cyclic Case

We are well prepared to start the meal which will culminate in the description of the fixed point free automorphism groups of abelian groups. We will reach our aim in 3 levels of increasing difficulty, namely dealing with cyclic, elementary abelian and abelian groups, refining our methods but unfortunately loose in completeness what we gain in generality of our results.

Antipasto: We give all fixed point free automorphism groups on the cyclic group Z_n.

4.1. Proposition. There is exactly one fixed point free automorphism group of order k on Z_{p^d}, p an odd prime, for $k|p-1$ and it is cyclic.

There is no fixed point free automorphism group of order k if $k \nmid p-1$.

Proof. Suppose $\alpha_i : x \mapsto ix \bmod p^d$ has a fixed point $x \in Z_{p^d}$, that is $\alpha_i(x) = ix = x$. Thus $ix - x = 0$ and $(i-1)x = 0 \bmod p^d$. If $\gcd(i-1, p) = 1$, then $i-1$ has a multiplicative inverse in Z_{p^d} resulting in $x = 0$, and α_i is fixed point free.

If, on the other hand, $i - 1 = lp$ for some l then $(i-1)y = lpy = 0 \bmod p^d$ holds for $y = p^{d-1} \neq 0$ and $\alpha_{lp+1}, l \in Z_{p^d}$, has a non trivial fixed point.

Now let

$$\begin{aligned} I &:= \{lp + 1 \bmod p^d : l \in Z_{p^d}\} \\ &= \{1, p+1, 2p+1, \dots, (p^{d-1}-1)p+1\}. \end{aligned}$$

As for $i, j \in I$ also $ij \bmod p^d \in I$ we have

$$U := \{\alpha_i : i \in I\} \leq \operatorname{Aut}(Z_{p^d})$$

and $|U| = |I| = p^{d-1}$. The elements of U are exactly the automorphisms on Z_{p^d} with fixed points.

So for $\Phi \leq \operatorname{Aut}(Z_{p^d})$ if and only if $|\Phi| = k$ with $k|p-1$, then $\Phi \cap U = \{\mathrm{id}\}$ and Φ is fixed point free on Z_{p^d}.

Since $\operatorname{Aut}(Z_{p^d})$ is cyclic by Proposition 1.17, there is exactly one subgroup of order k for each divisor k of $|\operatorname{Aut}(Z_{p^d})|$ and all subgroups are cyclic. □

4.2. Proposition. ([**KK95**] (3.2)) Let $G = \bigoplus_{i=1}^m Z_{p_i^{d_i}}, p_i$ distinct primes, be cyclic. The fixed point free automorphism groups of size k on G are of the form $\Phi = \langle(\alpha_1, \dots, \alpha_m)\rangle$, where α_i is an automorphism of $Z_{p_i^{d_i}}$ of order k for $i = 1, \dots, m$.

For each integer k satisfying $k|(p_i - 1)$ for all $1 \leq i \leq m$ there are exactly $(\phi(k))^{m-1}$ distinct, i.e., non-conjugated, fixed point free automorphism groups of size k on G.

Proof. If G has a cyclic 2-Sylow subgroup Z_{2^d}, then G has a unique element of order 2 and this has to be fixed by any automorphism of G. Thus G only permits the trivial fixed point free automorphism group of size 1.

We assume all p_i for $1 \leq i \leq m$ are odd. By Proposition 1.17 and Proposition 1.18, we have

$$\mathrm{Aut}(G) \cong \bigoplus_{i=1}^{m} (Z_{p_i-1} \times Z_{p_i^{d_i-1}}).$$

Let $\Phi < \mathrm{Aut}(G)$ of order k be fixed point free on G. Since Φ is fixed point free on each $Z_{p_i^{d_i}}$, by Proposition 4.1 we can embed Φ into $\bigoplus_{i=1}^{m} Z_{p_i-1}$, and

$$\Phi = \langle(\alpha_1, \dots, \alpha_m)\rangle$$

with $\alpha_i \in \mathrm{Aut}(Z_{p_i^{d_i}})$ of order k.

The assertion on the number of distinct fixed point free automorphism groups of a given size k follows since for all j_i such that $\gcd(j_i, k) = 1$ the groups $\langle(\alpha_1, \dots, \alpha_m)\rangle$ and $\langle(\alpha_1, \alpha_2^{j_2} \dots, \alpha_m^{j_m})\rangle$ are distinct. □

Note that for an arbitrary group with cyclic 2-Sylow subgroup there is no non trivial fixed point free automorphism group. According to Proposition 3.3, if an arbitrary group G has a characteristic subgroup or factor group which is cyclic, then G admits only cyclic fixed point free automorphism groups of a size given by Proposition 4.2.

CHAPTER 5

The Elementary Abelian Case

Primo Piatto: We obtain a result from Ke and Kiechle in [**KK95**] characterizing the cyclic fixed point free automorphism groups on elementary abelian groups by using a slightly different approach and notation. This enables us to give an assertion on the number of the cyclic, as well as a mean to describe the quaternion fixed point free automorphism groups and those of type (I).

According to Proposition 2.6 we identify the elementary abelian group $(G, +)$ of order p^n as n-dimensional vector space over the field F_p; an automorphism α on G can be regarded as regular F_p-linear transformation, i.e., induced by multiplication with a matrix $A \in GL(n, F_p)$ with respect to a basis $\mathcal{B}$ of G. We write $[\alpha]_{\mathcal{B}} = A$ and $\alpha(g) = Ag$ for the canonical basis $\mathcal{B}$ (see Proposition 2.8).

Recall that α being fixed point free is equivalent to A not having eigenvalue 1.

1. Cyclic Φ

5.1. Lemma. Let h be a monic irreducible polynomial of degree n over F_p and let $T : F_p^n \to F_p^n$ be defined by multiplication by $A = C(h)$, i.e., $T(v) = Av$. Then $\langle T \rangle$ is a fixed point free automorphism group on F_p^n of order $k = \mathrm{ord}(f)$ and $k | p^n - 1$.

Proof. Let $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ denote the vector with 1 in the i-th position and 0 elsewhere in F_p^n. Obviously $\mathcal{B} = \{e_1, \dots, e_n\}$ is a basis of F_p^n. Now identify F_p^n and $F_p[x]/\langle h \rangle$ as n-dimensional vector spaces over the field F_p via the vector space isomorphism

$$\begin{array}{rcl} \mu : F_p^n & \to & F_p[x]/\langle h \rangle \\ \sum_{i=1}^n a_i e_i & \mapsto & \sum_{i=1}^n a_i x^{i-1}. \end{array}$$

Then, from the definition of $A = C(h)$, we see that in $F_p[x]/\langle h \rangle$ the linear transformation T simply becomes $\bar{T} := \mu T \mu^{-1}$ and

$$\bar{T} : f \mapsto xf \bmod h,$$

and the order of T equals the order of h, i.e., the smallest natural number k such that $h | x^k - 1$.

Suppose there is some non trivial $f \in F_p[x]/\langle h \rangle$, and there is a natural number l such that $x^l f = f \bmod h$, thus

$$(x^l - 1) f = 0 \bmod h.$$

Since h is irreducible over F_p and $h \nmid f$, we necessarily have $h | x^l - 1$. Now $k | l$ and $\bar{T}^l = \mathrm{id}$.

So $\langle \bar{T} \rangle$ is fixed point free on $F_p[x]/\langle h \rangle$ as well as $\langle T \rangle$ is fixed point free on F_p^n. □

The following proposition is the fundamental result of this section. Notation and proof differs from the original work from Ke and Kiechle.

5.2. Proposition ([KK95](2.2)). Let $(G, +)$ be an elementary abelian group of order p^n with fixed point free automorphism group $\langle\varphi\rangle$ of order k where $\varphi(g) = Ag$ for all $g \in G$. Then there is a smallest natural number e such that $k|p^e - 1$ and $e|n$. Let $d = n/e$. Then there are monic irreducible polynomials h_i of degree e and order k over F_p for $i = 1, \ldots, d$ such that

$$A \simeq C(h_1) \oplus \cdots \oplus C(h_d)$$

Every automorphism of the form given above generates a fixed point free automorphism group on G.

Proof. Since $\langle\varphi\rangle$ is fixed point free on G, $k|p^n - 1$ by Proposition 3.1. The minimal polynomial m_φ of φ divides $x^k - 1$. By definition, every monic irreducible polynomial $h \in F_p[x]$, whose order divides k, is a divisor of $x^k - 1$.

Suppose there is a polynomial h such that $h^2|x^k - 1$. This implies that h divides the derivative of $x^k - 1$ as well, that is, $h|kx^{k-1}$. Since $\gcd(p, k) = 1$, we have $kx^{k-1} \neq 0$ and h is constant because $x^k - 1$ and kx^{k-1} are relatively prime.

Thus $x^k - 1$ actually equals the product of all distinct monic irreducible polynomials such that their orders divide k. Now evidently,

$$m_\varphi = \prod_{i=1}^{s} h_i$$

is the minimal polynomial of φ where h_i are distinct monic irreducible polynomials with orders dividing k for $i = 1, \ldots, s$ and

$$c_\varphi = \prod_{i=1}^{s} h_i^{n_i}$$

is the characteristic polynomial with integers n_i. By definition, each elementary divisor of φ is a power of some irreducible polynomial and has to divide m_φ. So the set of elementary divisors of φ is just the set of irreducible divisors of c_φ where each h_i occurs with multiplicity n_i. By Theorem 2.19

$$A \simeq \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{n_i} C(h_i).$$

Suppose there is a factor h_g of m_φ such that $h_g|x^l - 1$ for $l < k$. Since $C(h_i)$ is a root of h_i for each $i = 1, \ldots, s$ and especially $h_g(C(h_g)) = 0$, we get $C(h_g)^l - I = 0$. Then

$$A^l \simeq \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{n_i} C(h_i)^l$$

has the eigenvalue 1 and φ^l is not fixed point free, contrary to our assumption. Thus the order of h_i equals k for each $i = 1, \ldots, s$ and by Lemma 2.23 the degree of h_i equals e, where e is the smallest natural number such that $k|p^e - 1$ for each $i = 1, \ldots, d$. Thus the assertion on φ holds.

Define $\varphi : G \to G$ by multiplication with

$$A = C(h_1) \oplus \cdots \oplus C(h_d),$$

i.e., $\varphi(g) = Ag$, with the polynomials h_i of equal degree e and order k. Obviously $G = \bigoplus_{i=1}^{d} G_i$ where $G_i \cong Z_p^e$ are φ-invariant subspaces of G for $i = 1, \dots, n/e$.

Let $\varphi_i : G_i \to G_i$ be defined by multiplication by $C(h_i)$. Then the previous Lemma 5.1 can be applied to prove that $\langle \varphi_i \rangle$ is fixed point free on G_i. Since all restrictions φ_i on G_i are of the same order k, Proposition 3.3 (b) implies that $\langle \varphi \rangle$ is fixed point free on G. □

5.3. Corollary. (**[KK95]**(2.4)) Two automorphisms φ_1 and φ_2 both generating a fixed point free automorphism group on G are conjugate if and only if $c_{\varphi_1} = c_{\varphi_2}$.

Proof.

(a) If φ_1 and φ_2 are conjugate, then their characteristic polynomials are equal.
(b) Let φ_1 and φ_2 both generate a fixed point free automorphism group on G and let $c_{\varphi_1} = c_{\varphi_2} = h_1 \cdots h_d$. By Proposition 5.2 their elementary divisors and their rational canonical form coincide. Thus φ_1 and φ_2 are conjugate.

□

5.4. Corollary. Let $(G, +)$ be an elementary abelian group of order p^n. There is a cyclic fixed point free automorphism group of order k on G if and only if $k | p^n - 1$.

Proof.

(a) $k | p^n - 1$ is a necessary condition on G for having a fixed point free automorphism group of order k by Proposition 3.1.
(b) If $k | p^n - 1$ then $\exists \alpha \in F_{p^e}$ a primitive k-th root of unity over F_p with e the smallest natural number such that $k | p^e - 1$. Obviously $e | n$ and the minimal polynomial m_α of α over F_p is of degree e and order k. Now Proposition 5.2 applies to give a fixed point free automorphism group of order k.

□

Proposition 5.2 and its corollaries complete our task of fully characterizing the cyclic fixed point free automorphism groups on elementary abelian groups up to conjugacy.

We can construct all cyclic fixed point free automorphism groups of order k on Z_p^n by simply determining all irreducible polynomials of order k over F_p, choosing some h_i of them with multiplicity n_i as elementary divisors and applying Proposition 5.2.

If we look at φ generating a fixed point free automorphism group on G in a different way, we can gather even further insight.

5.5. Corollary. Let $(G, +)$ be an elementary abelian group of order p^n with fixed point free automorphism group $\langle \varphi \rangle$ of order k where $\varphi(g) = Ag$. Then there is a smallest natural number e such that $k | p^e - 1$ and the matrix A can be diagonalized over the extension field F_{p^e}.

$$A \simeq \bigoplus_{i=1}^{n/e} \operatorname{diag}(\alpha_i, \alpha_i^p, \alpha_i^{p^2}, \dots, \alpha_i^{p^{e-1}}),$$

where α_i is a primitive k-th root of unity for $i = 1, \dots, n/e$ and

$$\varphi \simeq \varphi^p \simeq \varphi^{p^2} \simeq \dots \simeq \varphi^{p^{e-1}}.$$

Proof. We may assume that

$$A = \bigoplus_{i=1}^{n/e} C(h_i)$$

by Proposition 5.2. For each $i = 1, \dots , n/e$ we consider $C(h_i)$ as matrix over some extension field K of F_p. According to Corollary 2.20 the matrix $C(h_i)$ of order k is diagonalizable over K if only $x^k - 1$ has k distinct roots in K.

In general, the splitting field of $x^k - 1$ over F_p is called the k-th *cyclotomic field* over F_p and since $\gcd(p, k) = 1$, all the roots of $x^k - 1$ are distinct. Note that $x^k - 1$ and its derivative kx^{k-1} have no common roots.

According to Theorem 2.47(ii) in [**LN84**] the k-th cyclotomic field over F_p is isomorphic to F_p^e, where e is the smallest natural number such that $k|p^e - 1$.

So by choosing F_p^e for K, all conditions for Corollary 2.20 are fulfilled. The roots of h_i are of the form $\alpha_i, \alpha_i^p \dots , \alpha_i^{p^{e-1}}$ for some $\alpha_i \in F_{p^e}$, they are all distinct and have multiplicative order k. Thus

$$C(h_i) \simeq \operatorname{diag}(\alpha_i, \alpha_i^p \dots , \alpha_i^{p^{e-1}})$$

and obviously,

$$C(h_i) \simeq C(h_i)^p \simeq \dots C(h_i)^{p^{e-1}}$$

over F_{p^e} for each $i = 1, \dots , n/e$.

Naturally, the characteristic polynomial of φ is the same, whether A is considered over F_p or over its extension, i.e.,

$$c_\varphi = c_A = \prod_{i=1}^{n/e} \prod_{j=0}^{e-1} (x - \alpha_i^{p^j})$$

and since

$$c_A = c_{A^p} = \dots = c_{A^{p^{e-1}}}$$

Corollary 5.3 implies

$$\varphi \simeq \varphi^p \simeq \varphi^2 \simeq \dots \simeq \varphi^{p^{e-1}}$$

and the assertion is proven. □

If φ generates a fixed point free automorphism group on G of order k and $k|p - 1$, i.e., $e = 1$, then A can be diagonalized over F_p and the statements of Proposition 5.2 and Corollary 5.5 coincide.

5.6. Lemma. Let $(G, +)$ be an elementary abelian group of order p^n with fixed point free automorphism group $\langle\varphi\rangle$ of order k and let $1 < r < k$. Then

$$\varphi \simeq \varphi^r$$

if and only if

$$c_\varphi = \prod_{i=1}^{n/d} [(x - \alpha_i)(x - \alpha_i^r) \cdots (x - \alpha_i^{r^{d-1}})]$$

in $F_p[x]$, where d is the smallest natural number such that $k|r^d-1$. Also $d| \gcd(n, \phi(k))$ and $d > 1$.

Proof. Let $\varphi : g \mapsto Ag$. According to Corollary 5.5 the matrix A can be diagonalized over the field F_{p^e}, where e is the smallest natural number such that $k|p^e - 1$. Let $\bar{A}$ denote the diagonalization of A,

$$\bar{A} = \bigoplus_{i=1}^{s} \alpha_i I_{n_i},$$

where $n = \sum_{i=1}^{s} n_i$ and the $\alpha_i \in F_{p^e}$ are distinct primitive k-th roots of $x^k - 1$.

We notice $A \simeq A^r \simeq A^{r^2} \simeq \ldots \simeq A^{r^{d-1}}$, where d is the smallest natural number such that $k|r^d - 1$, to be conjugate,

$$\bar{A}^{r^j} = \bigoplus_{i=1}^{s} \alpha_i^{r^j} I_{n_i},$$

and therefore the multiplicity n_i of the eigenvalue α_i of $\bar{A}$ equals the multiplicity of $\alpha_i^{r^j}$ for $j = 1, \ldots, d-1$ as eigenvalue of $\bar{A}$. Necessarily, d divides n and $d > 1$ since $k \nmid r - 1$. Moreover, $\langle r \rangle$ is a subgroup of Z_k^* of order d, thus $d|\phi(k)$.

Conversely, if the automorphism $\varphi : g \mapsto Ag$ has a characteristic polynomial as given above, then A can be diagonalized,

$$A \simeq \bigoplus_{i=1}^{n/d} \operatorname{diag}(\alpha_i, \alpha_i^r \ldots \alpha_i^{r^{m-1}}),$$

over F_{p^e} and since $A \simeq A^r$, also $\varphi \simeq \varphi^r$. □

Computing the number of non conjugate automorphisms of a given order k generating a fixed point free automorphism group on G is just a combinatorial problem, because of Proposition 5.2, depending on the number of distinct monic irreducible polynomials in $F_p[x]$ of order k. But in order to find the number of non conjugated cyclic fixed point free automorphism groups of size k, we need a more general view and some new definitions. Even before this we have this simple lemma for motivation.

5.7. Lemma. Let φ be an automorphism of order k on G. If $\varphi^r \simeq \varphi$ for all $r \in S \subseteq \{1, \ldots, k-1\}$, then $\varphi^r \simeq \varphi$ for all $r \in \langle S \rangle \leq Z_k^*$.

Proof. Let $i, j \in S$. Then $\varphi^{ij} = (\varphi^i)^j \simeq \varphi^j \simeq \varphi$. □

5.8. Definition. For a fixed k let R denote the set of rational canonical forms for automorphisms φ, which generate a fixed point free automorphism group of order k on G, i.e., R is a set of representatives for each conjugacy class of automorphisms of order k.

For an arbitrary subgroup $U \leq Z_k^*$, let

$$R_U = \{\varphi \in R : \varphi^r \simeq \varphi, \forall r \in U\}.$$

Let $\langle p \rangle = \{1, p, p^2, \ldots, p^{e-1}\} \leq Z_k^*$ where e is the smallest natural number such that $k|(p^e - 1)$ be denoted by E. Then obviously,

$$R_E = R$$

by Proposition 5.5.

The sets R_U give a classification of the mappings φ and their cardinality is easy to determine.

5.9. Lemma. Let φ be an automorphism of order k on Z_p^n.

$$\varphi \in R_U \quad \Leftrightarrow \quad c_\varphi = \prod_{i=1}^{n/|\langle E,U\rangle|} \prod_{j\in\langle E,U\rangle} (x-\alpha_i^j) \text{ in } F_p[x],$$

where α_i are primitive k-th roots of unity over F_p.

Proof. If $\varphi \in R_U$, then for every root $\alpha_i \in F_{p^e}$ of c_φ also α_i^r for $r \in U$ has to be a root of c_φ with equal multiplicity for the same reason as in the proof of Corollary 5.5. Thus c_φ is of the given form.

The converse is trivial. □

Now we are using this characterization for counting the elements of R_U.

5.10. Lemma.

$$|R_U| = \begin{cases} \begin{pmatrix} \frac{\phi(k)}{|\langle E,U\rangle|} + \frac{n}{|\langle E,U\rangle|} - 1 \\ \frac{n}{|\langle E,U\rangle|} \end{pmatrix} & \text{if } |\langle E,U\rangle| \text{ divides } n \\ 0 & \text{else} \end{cases}$$

Proof. By Lemma 5.9 we have the characteristic polynomial of φ in R_U as product of $n/|\langle E,U\rangle|$ factors $\prod_{j\in\langle E,U\rangle}(x-\alpha_i^j)$. Thus $t := |\langle E,U\rangle|$ has to divide n.

There are exactly $\phi(k)$ distinct primitive roots of $x^k - 1 = 0$ in F_{p^e} and they are separated into disjoint sets

$$\{\alpha_i^j : j \in \langle E,U\rangle\}$$

of size t. We get all distinct polynomials c_φ by choosing n/t of these $\phi(k)/t$ sets and make their elements roots of c_φ. There are exactly

$$\binom{\phi(k)/t + n/t - 1}{n/t}$$

possibilities to do this. □

We get the number of non conjugated φ as a corollary.

5.11. Proposition. Let $(G,+)$ be an elementary abelian group of order p^n. If $k|p^n-1$, then there is a smallest natural number e such that $k|p^e-1$ and there are exactly

$$|R| = \binom{\phi(k)/e + n/e - 1}{n/e}$$

non conjugate automorphisms on G which generate a fixed point free automorphism group of order k.

Proof. Since $R = R_E$ and $|E| = e$ the number $|R|$ follows immediately from Lemma 5.10. □

We also note the fact that if $\varphi \in R_U$ and for all W such that $U < W \leq Z_k^*$ it holds that $\varphi \notin R_W$, then the group $\langle\varphi\rangle$ has exactly

$$[Z_k^* : \langle E,U\rangle] = \frac{\phi(k)}{|\langle E,U\rangle|}$$

non conjugate generators.

Hence we get the following formula:

5.12. Proposition. Let $\mathcal{U} = \{U \leq Z_k^* : E \leq U\}$. There are exactly

$$\mathcal{N}_k = \frac{1}{\phi(k)} \sum_{U \in \mathcal{U}} |U|(|R_U| - |\bigcup_{W>U} R_W|)$$

non conjugate cyclic fixed point free automorphism groups of order k on $G = Z_p^n$.

Proof.

$$|R_U| - |\bigcup_{W>U} R_W|$$

gives the number of non conjugate $\varphi \in R_U$ for which there are exactly $|U|$ powers $\varphi^r \simeq \varphi$. Thus every $\phi(k)/|U|$ of these non conjugate φ generate conjugate groups $\langle\varphi\rangle$. By summing up over all $U \leq Z_k^*$ with $E \leq U$ we are done. □

The disadvantage of this expression is plainly visible. While we know $|R_U|$ by Lemma 5.10, the evaluation of $|\bigcup_{W \in \mathcal{U}, W>U} R_W|$ in general involves some tedious computation. However, it is merely a problem of knowing the subgroup lattice of the abelian group Z_k^* (see Proposition 1.18). For the solution we refer to the next chapter on abelian groups where the same problem is dealt with more generally.

5.13. Example. We would like to apply our new knowledge and determine all cyclic fixed point free automorphism groups of order 8 on Z_5^4 up to conjugacy.

We need irreducible polynomials of order 8 over F_5. Since $8|5^2 - 1$ we know that the degree of such polynomials has to be 2 and since $\phi(8) = 4$ we know that there are exactly 2 such polynomials h_1, h_2. We look for them among the factors of

$$x^8 - 1 = (x+1)(x+2)(x+3)(x+4)(x^2+2)(x^2+3)$$

and find $h_1 = x^2 + 2$ and $h_2 = x^2 + 3$ of order 8. By Proposition 5.2 and Corollary 5.3 the matrices $A = C(h_1) \oplus C(h_1), B = C(h_1) \oplus C(h_2)$ and $C = C(h_2) \oplus C(h_2)$ all induce non conjugate fixed point free automorphisms φ_1, φ_2 and φ_3, respectively, of order 8 on Z_5^4. The characteristic polynomials are

$$c_{\varphi_1} = (x^2+2)^2 = (x-\alpha)^2(x-\alpha^5)^2,$$

$$c_{\varphi_2} = (x^2+2)(x^2+3) = (x-\alpha)(x-\alpha^3)(x-\alpha^5)(x-\alpha^7).$$

$$c_{\varphi_3} = (x^2+3)^2 = (x-\alpha^3)^2(x-\alpha^7)^2,$$

where α is a primitive 8-th root of unity over F_5. Proposition 5.11 reassures that there are exactly

$$\binom{4/2 + 4/2 + 1}{4/2} = 3$$

such non conjugate mappings. We see that $c_{\varphi_1^3} = c_{\varphi_3}$, i.e., $\langle\varphi_1\rangle \simeq \langle\varphi_3\rangle$ and there are only 2 non conjugated cyclic fixed point free automorphism groups of order 8, namely $\langle\varphi_1\rangle$ and $\langle\varphi_2\rangle$ with

$$\varphi_1(g) = \begin{pmatrix} 0 & 3 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 1 & 0 \end{pmatrix} g$$

and

$$\varphi_2(g) = \begin{pmatrix} 0 & 3 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 \end{pmatrix} g.$$

Without regard of this result we would also like to apply Proposition 5.12 and define $E = \{1, 5\} \leq Z_8^*$. By Proposition 1.17 we have $Z_8^* \cong Z_2^2$, thus $\mathcal{U} = \{E, Z_8^*\}$. We already computed

$$|R_E| = 3$$

and furthermore,

$$|R_{Z_8^*}| = \binom{4/4 + 4/4 - 1}{4/4} = 1.$$

There are exactly

$$\mathcal{N}_8 = \frac{1}{\phi(8)} \cdot \left[|E|(|R_E| - |R_{Z_8^*}|) + |Z_8^*|(|R_{Z_8^*}| - 0) \right] = 2$$

non conjugate cyclic fixed point free automorphism groups of order 8 on Z_5^4.

2. Quaternion Φ

By using the same principles as above we are now going to determine all the quaternion fixed point free automorphism groups on $G = Z_p^n$. We will need the following lemma first.

5.14. Lemma. Let e be the smallest natural number such that $2^t | p^e - 1$ for an odd prime p and $t > 1$. Then $e = 2^l$ for some l.

Proof. Suppose $e = 2^l r$ with r odd is the smallest natural number such that $2^t | p^e - 1$. Then

$$p^e - 1 = (p^{2^l} - 1)(p^{2^l (r-1)} + \ldots + p^{2^l} + 1),$$

and since p is odd and r is odd, the sum $\sum_{i=0}^{r-1} p^{2^l i}$ is odd. Thus $2^t | p^{2^l} - 1$ and $r = 1$. □

5.15. Lemma. Let $(G, +)$ be an elementary abelian group of order p^n with φ, ψ such that $\langle \varphi, \psi \rangle$ is a non cyclic fixed point free automorphism group on G with $\varphi^m = \psi^4 = id$, where either $m > 1$ is odd and $|\Phi| = 4m$ or $m = 2^t$ for $t \geq 2$ and Φ is a quaternion group of order 2^{t+1}. Let e be the smallest natural number such that $m | p^e - 1$.

(a) We have $\psi^{-1} \varphi \psi = \varphi^{-1}$.

(b) If $\varphi : g \mapsto Ag$ and $\psi : g \mapsto Bg$ for matrices A, B, then there is a matrix X over F_{p^e} such that

$$X^{-1}AX = \bigoplus_{i=1}^{n/2} \begin{pmatrix} \alpha_i & 0 \\ 0 & \alpha_i^{-1} \end{pmatrix}, X^{-1}BX = \bigoplus_{i=1}^{n/2} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

where $\alpha_i \in F_{p^e}$ are primitive m-th roots of unity for $i = 1, \ldots, n/2$.

(c) Any linear transformations φ, ψ fulfilling the above relations generate a fixed point free automorphism group of type (I) if m is odd and a quaternion fixed point free automorphism group of order 2^{t+1} if $m = 2^t$.

PROOF.

(a) Let m be odd. Then Φ has type I, $\Phi' = \langle\varphi\rangle$ and $\psi^{-1}\varphi\psi = \varphi^r$ where $\gcd(m, r-1) = 1$. Since $\psi^2(g) = -g$ for all $g \in G$, we have that ψ^2 commutes with φ,

$$\varphi = \psi^{-2}\varphi\psi^2 = \varphi^{r^2}.$$

Thus $m|r^2-1$ and $\gcd(m, r-1) = 1$ implies $m|r+1$, i.e., $r = m-1$.

If $m = 2^t$, then Φ is a quaternion group and $\psi^{-1}\varphi\psi = \varphi^{-1}$ follows directly from the presentation of Φ.

(b) Since φ and φ^{-1} are conjugate by (a), $c_\varphi = \prod_{i=1}^{n/2}(x-\alpha_i)(x-\alpha_i^{-1})$ by Lemma 5.6 and n has to be even. The matrix A can be diagonalized over F_{p^e}, where e is the smallest natural number such that $m|p^e-1$. Let n_i be the multiplicity of α_i as root of c_φ and let

$$\bar{A} = X^{-1}AX$$

denote the diagonalization of A with $X \in GL(n, F_{p^e})$,

$$\bar{A} = \bigoplus_{i=1}^{d} \begin{pmatrix} \alpha_i I_{n_i} & 0 \\ 0 & \alpha_i^{-1} I_{n_i} \end{pmatrix},$$

where $n/2 = \sum_{i=1}^{d} n_i$ and the $\alpha_i \in F_{p^e}$ are distinct primitive m-th roots of unity. Let

$$\bar{B} = X^{-1}BX.$$

Now if v is an element of the eigenspace V_{α_i} of $\bar{A}$ for the eigenvalue α_i, then

$$\bar{A}(\bar{B}v) = \bar{B}(\bar{B}^{-1}\bar{A}\bar{B})v = \bar{B}\bar{A}^{-1}v = \alpha_i^{-1}\bar{B}v$$

and the vector $\bar{B}v$ is an eigenvector of the matrix $\bar{A}$ for the eigenvalue α_i^{-1}, thus $\bar{B}v \in V_{\alpha_i^{-1}}$. Actually $\bar{B}$ defines an isomorphism between the eigenspaces V_{α_i} and $V_{\alpha_i^{-1}}$. Note that $\bar{B}^2 = -I$ and $\bar{B}(\bar{B}v) = -v \in V_{\alpha_i}$.

For $i = 1, \ldots, d$ let $\mathcal{B}_i = \{e_{i1}, \ldots, e_{in_i}\}$ be basis of V_{α_i}. Then $\{\bar{B}e_{i1}, \ldots, \bar{B}e_{in_i}\}$ is a basis of $V_{\alpha_i^{-1}}$ and hence the union of these $\mathcal{B}_i \cup \bar{B}(\mathcal{B}_i)$ over i, i.e., the ordered set

$$\mathcal{B} = \bigcup_{i=1}^{d} \{e_{i1}, \ldots, e_{in_i}\} \cup \{\bar{B}(e_{i1}), \ldots, \bar{B}(e_{in_i})\},$$

is a basis of $F_{p^e}^n$, for which $\bar{B}$ is of the form

$$\bar{B} = \bigoplus_{i=1}^{d} \begin{pmatrix} 0 & -I_{n_i} \\ I_{n_i} & 0 \end{pmatrix}$$

with $\sum_{i=1}^{d} n_i = n/2$. By rearranging the basis of $F_{p^e}^n$ we obtain the form given in the hypothesis for $\bar{A}$ and $\bar{B}$.

(c) By construction, $\langle\bar{A}, \bar{B}\rangle$ is a group of type (I) or a quaternion group and all elements are of the form $\bar{B}^i\bar{A}^j$ for $0 \le i \le 3$ and $0 \le j \le m-1$. Since neither

$$\bar{A}^j = -\bar{B}^2\bar{A}^j = \bigoplus_{i=1}^{n/2} \begin{pmatrix} \alpha_i^j & 0 \\ 0 & \alpha_i^{-j} \end{pmatrix}$$

for $1 \leq j \leq 2^t - 1$ nor

$$\bar{B}\bar{A}^j = -\bar{B}^3\bar{A}^j = \bigoplus_{i=1}^{n/2} \begin{pmatrix} 0 & -\alpha_i^{-j} \\ \alpha_i^j & 0 \end{pmatrix}$$

with characteristic polynomial $\prod_{i=1}^{n/2}(x^2+1) = (x^2+1)^{n/2} = c_{\bar{B}}$ has eigenvalue 1, any φ, ψ fulfilling the above conditions generate a fixed point free automorphism group on G indeed.

□

Lemma 5.15 describes fixed point free automorphism groups on G which are extensions of a cyclic group $\langle\varphi\rangle$ with a cyclic group $\langle\psi\rangle$ of order 4, thus both non cyclic fixed point free automorphism groups of type (I) with order $4m, m$ odd and quaternion groups of order 2^{t+1}. It states necessary conditions on φ, ψ, especially on the characteristic polynomial

$$c_\varphi = \prod_{i=1}^{n/2}(x-\alpha_i)(x-\alpha_i^{-1})$$

of φ. If the minimal polynomial m_α divides c_φ, then so does $m_{\alpha^{-1}}$. We have to distinguish 2 cases: either $m_\alpha \neq m_{\alpha^{-1}}$ and

$$c_\varphi = \prod_{i=1}^{n/2e} m_{\alpha_i} m_{\alpha_i^{-1}}$$

or $m_\alpha = m_{\alpha^{-1}}$ and

$$c_\varphi = \prod_{i=1}^{n/e} m_{\alpha_i}.$$

The next lemma characterizes the difference for the case of Φ being quaternion.

5.16. Lemma. Let α be a 2^t-th root of unity for $m > 1$ over F_p. Then $m_\alpha = m_{\alpha^{-1}}$, if and only if $2^t | p+1$ and $m_\alpha = (x-\alpha)(x-\alpha^{-1})$.

Proof. Since

$$m_\alpha = (x-\alpha)(x-\alpha^p)\cdots(x-\alpha^{p^{e-1}}),$$

where $e = 2^l$ is the smallest natural number such that $2^t | p^e - 1$, we have $m_\alpha = m_{\alpha^{-1}}$ if and only if

$$\alpha^{-1} \in \{\alpha, \alpha^p, \ldots, \alpha^{p^{e-1}}\}.$$

Thus $\alpha^{-1} = \alpha^{p^i}$ for some $1 \leq i \leq e-1$ and $2^t | p^i + 1$. Now $2^t | p^{2i} - 1$ and $e | 2i$. Because $i < e$ this results in $i = 2^{l-1}$. Suppose $i > 1$, then $4 | p^i - 1$ in contradiction to $2^t | p^i + 1$ for $m \geq 2$. Therefore $i = 1, e = 2$ and $p \equiv 3 \bmod 4$.

The converse is obvious. □

5.17. Proposition. Let $(G, +)$ be an elementary abelian group of order p^n and $2^t \nmid p+1$.

(a) There exists a quaternion fixed point free automorphism group Φ of order 2^{t+1} on G if and only if $2^{t+1} | p^n - 1$ and $2e | n$, where e is the smallest natural number such that $2^t | p^e - 1$.

(b) Any such Φ is conjugate to a group $\langle\varphi,\psi\rangle$ with $\varphi^{2^t} = \mathrm{id}, \psi^2 = \varphi^{2^{t-1}}$, $\psi^{-1}\varphi\psi = \varphi^{-1}$, where $\varphi : g \mapsto Ag, \psi : g \mapsto Bg$ and

$$A = \bigoplus_{i=1}^{n/e} \begin{pmatrix} C(h_i) & 0 \\ 0 & C(h_i)^{-1} \end{pmatrix}, B = \bigoplus_{i=1}^{n/e} \begin{pmatrix} 0 & -I_e \\ I_e & 0 \end{pmatrix},$$

and $h_1, \dots, h_d$ are monic irreducible polynomials of degree $e = 2^l$ and order 2^t over F_p.

(c) Any automorphisms φ, ψ fulfilling the above relations generate a quaternion fixed point free automorphism group of order 2^{t+1} on G.

Proof.

(a) If $2^{t+1} \nmid p^n - 1$, then there is no fixed point free automorphism group on G according to Proposition 3.1. By Lemma 5.15 there is no quaternion fixed point free automorphism group if $2 \nmid n$.

The converse can be seen by the construction in (b).

(b) Let $2^{t+1}|p^n - 1$ and $2e|n$. Suppose $\Phi = \langle\varphi,\psi\rangle$ is a quaternion fixed point free automorphism group of order 2^{t+1}. Lemma 5.15 and Lemma 5.16 give the characteristic polynomial

$$c_\varphi = \prod_{i=1}^{n/2e} (m_{\alpha_i} m_{\alpha_i^{-1}}),$$

where α_i is a primitive 2^t-th root of unity over F_p and m_{α_i} is its minimal polynomial of degree e. We define

$$A = \bigoplus_{i=1}^{n/2e} \begin{pmatrix} C(m_{\alpha_i}) & 0 \\ 0 & C(m_{\alpha_i})^{-1} \end{pmatrix}$$

and since

$$C(m_{\alpha_i})^{-1} \simeq \mathrm{diag}(\alpha_i^{-1}, \alpha_i^{-p}, \dots, \alpha_i^{-p^{e-1}}) \simeq C(m_{\alpha_i^{-1}})$$

over F_{p^e}, the characteristic polynomial $c_A = c_\varphi$. Thus we may assume $\varphi(g) = Ag$. Note that A is not the rational canonical form for φ but it serves our purpose better. By defining the matrix

$$B = \bigoplus_{i=1}^{n/2e} \begin{pmatrix} 0 & -I_e \\ I_e & 0 \end{pmatrix}$$

and the linear transformation $\psi^*(g) = Bg$ we obtain a quaternion fixed point free automorphism group $\langle\varphi,\psi^*\rangle$ of order 2^{t+1}. Since Lemma 5.15 allows for each choice of φ only one quaternion extension, it holds $\langle\varphi,\psi\rangle = \langle\varphi,\psi^*\rangle$ and, w.l.o.g., $\psi = \psi^*$.

(c) Follows from the construction in (b) and Lemma 5.15 (c).

□

We will need the following lemma to guarantee the existence of a quaternion fixed point free automorphism group of order 2^{t+1} if $m_\alpha = m_{\alpha^{-1}}$.

5.18. Lemma. For each element $a \in F_p$, for p prime, there are $u, v \in F_p$ such that $u^2 + v^2 = a$.

Proof. Let $S = \{u^2 : u \in F_p^*\}$ denote the set of squares in F_p^*.

Suppose $a = 0$ or $a = u^2 \in S$. Then the hypothesis is fulfilled for $u = v = 0$ or $v = 0$ respectively.

Suppose for all $u, v \in F_p$ we have that $u^2 + v^2 \in S$. For $n \in S$ we have $n+1 \in S$ since $1 \in S$. By induction $S = F_p^*$ which is obviously false. Thus there are $u, v \in F_p$ and $l \in F_p^* \setminus S$ such that $u^2 + v^2 = l$.

Since $\{lt^2 : t \in F_p^*\} = F_p^* \setminus S$ and $(ut)^2 + (vt)^2 = lt^2$, all non square elements of F_p can be represented as sum of two squares. □

Here is the result corresponding to Proposition 5.17.

5.19. Proposition. Let $(G, +)$ be an elementary abelian group of order p^n and let $2^t | p+1$.

(a) There exists a quaternion fixed point free automorphism group Φ of order 2^{t+1} on V if and only if $2|n$.

(b) Any such Φ is conjugate to a group $\langle \varphi, \psi \rangle$ with $\varphi^{2^t} = \mathrm{id}, \psi^2 = \varphi^{2^{t-1}}$, $\psi^{-1}\varphi\psi = \varphi^{-1}$ where $\varphi : g \mapsto Ag, \psi : g \mapsto Bg$ and
$$A = \bigoplus_{i=1}^{n/2} \begin{pmatrix} 0 & -1 \\ 1 & a_i \end{pmatrix}, B = \bigoplus_{i=1}^{d} \begin{pmatrix} u_i & v_i \\ v_i - u_i a_i & -u_i \end{pmatrix},$$
and $x^2 - a_i x + 1$ is irreducible of order 2^t over F_p and $u_i^2 + v_i^2 - u_i v_i a_i + 1 \equiv 0 \bmod p$.

(c) Any linear transformations φ, ψ fulfilling the above relations generate a fixed point free quaternion automorphism group of order 2^{t+1} on G.

Proof.

(a) If $2 \nmid n$, then $2^{t+1} \nmid p^n - 1$ and there is no quaternion fixed point free automorphism group on G according to Proposition 3.1 and Lemma 5.15. The converse is proven by (b).

(b) Let $2|n$. Since $2^{t+1}|(p-1)(p+1)$ also $2^{t+1}|p^n - 1$. Suppose $\Phi = \langle \varphi, \psi \rangle$ is a quaternion fixed point free automorphism group of order 2^{t+1}.

Lemma 5.15 and Lemma 5.16 provide the characteristic polynomial
$$c_\varphi = \prod_{i=1}^{n/2} (x - \alpha_i)(x - \alpha_i^{-1}) = \prod_{i=1}^{n/2} m_{\alpha_i}$$
where α_i is a primitive 2^t-th root of unity over F_p and
$$m_{\alpha_i} = (x - \alpha_i)(x - \alpha_i^{-1}) = x^2 - a_i x + 1$$
for $a_i \in F_p$ is its minimal polynomial of degree 2.

By Proposition 5.2 we may assume
$$A = \bigoplus_{i=1}^{n/2} C(m_{\alpha_i}) = \bigoplus_{i=1}^{n/2} \begin{pmatrix} 0 & -1 \\ 1 & a_i \end{pmatrix}.$$

Let
$$X = \begin{pmatrix} 0 & -1 \\ 1 & a \end{pmatrix}$$

and $x^2 - ax + 1$ be of order 2^t over F_p. Now suppose there is a 2×2 matrix

$$Y = \begin{pmatrix} u & v \\ w & y \end{pmatrix}$$

over F_p such that $Y^2 = -I$ and $Y^{-1}XY = X^{-1}$. Since

$$Y^2 = \begin{pmatrix} u^2 + vw & v(u+y) \\ w(u+y) & wv + y^2 \end{pmatrix},$$

we have either $u + y = 0$ or $v = w = 0$. The latter results in $u^2 = y^2 = -1$ thus the polynomial x^2+1 splits into 2 linear factors over F_p which is possible if and only if $4|p-1$, contrary to $2^t|p+1$ for $m > 1$. Hence $y = -u$ and $u^2 + vw = -1$. Next we use the equality

$$\begin{aligned} XY &= YX^{-1} \\ \begin{pmatrix} 0 & -1 \\ 1 & a \end{pmatrix}\begin{pmatrix} u & v \\ w & -u \end{pmatrix} &= \begin{pmatrix} u & v \\ w & -u \end{pmatrix}\begin{pmatrix} a & 1 \\ -1 & 0 \end{pmatrix} \\ \begin{pmatrix} -w & u \\ u + wa & v - ua \end{pmatrix} &= \begin{pmatrix} ua - v & u \\ wa + u & w \end{pmatrix} \end{aligned}$$

and find $w = v - ua$. Thus for

$$Y = \begin{pmatrix} u & v \\ v - ua & -u \end{pmatrix}$$

with $u^2 + v^2 - uva = -1$ the group $\langle X, Y\rangle$ is a quaternion group of order 2^t. By Lemma 5.15 (c) none of its elements except I has 1 as eigenvalue.

For the existence of Y we have to show that if $x^2 - ax + 1 = 0$ has no roots in F_p, the equation

$$x^2 + y^2 - axy + 1 = 0$$

has solutions $x = u, y = v$ in F_p. We rewrite

$$\begin{aligned} y_{1,2} &= \frac{ax}{2} \pm \sqrt{\frac{a^2x^2}{2^2} - 1 - x^2} \\ &= \frac{ax}{2} \pm x\sqrt{\frac{a^2}{4} - x^{-2} - 1} \end{aligned}$$

which is solvable if and only if $\frac{a^2}{4} - 1 - x^{-2}$ is a square in F_p, i.e., there is $z \in F_p$ such that

$$(x^{-1})^2 + z^2 = \frac{a^2}{4} - 1.$$

Lemma 5.18 gives this assertion and guarantees the existence of a matrix Y for each X which fulfill the above conditions.

By defining the matrix

$$B = \bigoplus_{i=1}^{n/2} \begin{pmatrix} u_i & v_i \\ v_i - u_i a_i & -u_i \end{pmatrix}$$

with $u_i^2 + v_i^2 - u_i v_i a_i + 1 \equiv 0 \bmod p$ and $\psi^* : g \mapsto Bg$, we obtain a quaternion fixed point free automorphism group $\langle \varphi, \psi^*\rangle$ of order 2^{t+1}. By Lemma 5.15 it holds $\langle \varphi, \psi\rangle = \langle \varphi, \psi^*\rangle$ and, w.l.o.g., $\psi = \psi^*$.

(c) It is easy to see that no non trivial element of the automorphism group constructed in (b) admits the eigenvalue 1.

□

By Proposition 5.17 and Proposition 5.19, respectively, we have characterized all quaternion fixed point free automorphism groups on $G = Z_p^n$ up to conjugacy. We add an assertion on the number of such groups.

5.20. Proposition. Let $\mathcal{U} = \{U \leq Z_{2^t}^* : \langle p, -1\rangle \leq U\}$ and let R_U denote the set of non conjugate automorphisms φ generating a fixed point free automorphism group of order 2^t on Z_p^n such that $\varphi^r \simeq \varphi$ for all $r \in U$. Then there are exactly

$$\frac{1}{2^{t-1}} \sum_{U \in \mathcal{U}} |U|(|R_U| - |\bigcup_{W > U} R_W|)$$

non conjugate quaternion fixed point free automorphism groups of order $2^m + 1$ on Z_p^n.

Proof. This follows from Proposition 5.10 and Lemma 5.17. □

5.21. Corollary. All quaternion fixed point free automorphism groups of order 8 on $G = Z_p^n$ are conjugated.

Proof. This is a simple consequence of Lemma 5.16 and the fact that there are exactly 2 primitive 4-th roots of unity over F_p. □

5.22. Example. We give the quaternion fixed point free automorphism groups on Z_5^4 and refer to the previous example where we determined the automorphisms of order 8.

2 and 3 are 4-th primitive roots over F_5; $x + 3$ and $x + 2$ are the polynomials of order 4 over F_5. Thus by Lemma 5.15 or Proposition 5.17 we have that $\langle \varphi, \psi \rangle$ where $\varphi : g \mapsto Ag, \psi : g \mapsto Bg$ and

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \oplus \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix},$$

$$B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

is a quaternion fixed point free automorphism group of order 8 and it is unique up to conjugacy according to Corollary 5.21.

Since $\langle 5, -1\rangle = Z_8^*$, the formula of Proposition 5.20 shows that there is exactly 1 quaternion fixed point free automorphism group of order 16 up to conjugacy. $x^2 + 2$ is a polynomial of order 8 over F_5. By Proposition 5.17 the matrices

$$A = \begin{pmatrix} 0 & 3 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 \end{pmatrix},$$

$$B = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

induce automorphisms $\varphi : g \mapsto Ag, \psi : g \mapsto Bg$ so that $\langle \varphi, \psi \rangle$ is such a group.

3. Φ of Type (I)

Next we dedicate ourselves to fixed point free automorphism groups of type (I) and give a necessary condition for their existence on Z_p^n.

5.23. Lemma. Let $(G,+)$ be an elementary abelian group of order p^n, let Φ be a non cyclic fixed point free automorphism group on G with cyclic Sylow subgroups, i.e., $\Phi = \langle \varphi, \psi \rangle$ where $\varphi^s = \psi^t = \mathrm{id}, \psi^{-1}\varphi\psi = \varphi^r$ and $r^t \equiv 1(s), \gcd(s, t(r-1)) = 1$ and $|\Phi| = st$.

Let d be the smallest natural number such that $s|r^d - 1$. Then $d|\gcd(n, \phi(s), t)$ and $d > 1$.

Proof. By Lemma 5.6 we have $d|\gcd(n, \phi(s))$ and $d > 1$. Since $s|r^t - 1$, it also holds $d|t$. □

5.24. Corollary. Let $(G,+)$ be an elementary abelian group of order p^n. If $\gcd(n, p^n - 1) = 1$, then every fixed point free automorphism group Φ on G is cyclic.

Proof. Suppose there is a quaternion fixed point free automorphism group on G. Then n has to be even by Lemma 5.15 but since $\gcd(n, p^n - 1) = 1$, we are forced to conclude that $|G| - 1$ is odd and there is no fixed point free automorphism of even order.

Suppose there is a group $\Phi = \langle \varphi, \psi \rangle$ as defined in Lemma 5.23. Then $\gcd(n, t) > 1$ is in contradiction to $t|p^n - 1$, and hence $\gcd(n, p^n - 1) = 1$. □

We give the fixed point free automorphism groups on Z_p^n, where n is prime.

5.25. Proposition. Let $(G,+)$ be an elementary abelian group of order p^n with n prime and let there is a fixed point free automorphism group $\Phi = \langle \varphi, \psi \rangle$ on G where $\varphi^s = \psi^t = \mathrm{id}, \psi^{-1}\varphi\psi = \varphi^r$ and $r^t \equiv 1(s), \gcd(s, t(r-1)) = 1$ and $|\Phi| = st$.

Then $n|p - 1, s|r^n - 1$ and $n^2|t$. If $\varphi : g \mapsto Ag$ and $\psi : g \mapsto Bg$ for matrices A, B, then there is a matrix X over F_{p^n} such that

$$X^{-1}AX = \mathrm{diag}(\alpha, \alpha^r, \ldots, \alpha^{r^{n-1}}), X^{-1}BX = C(x^n - b)$$

where $\alpha \in F_{p^n}$ is a primitive s-th roots of unity and $b^{t/n} = 1$.

Proof. Since $\varphi \simeq \varphi^r \simeq \ldots \varphi^{r^{t-1}}$ and n is prime, Lemma 5.6 implies that $c_{varphi} = \prod_{i=1}^n (x - \alpha^i)$ for α a primitive s-th root of unity. Let e be the smallest natural number such that $s|p^e - 1$, then $e \in \{1, n\}$. Let $\bar{A} = X^{-1}AX$ denote the diagonalization of A over F_{p^e},

$$\bar{A} = \mathrm{diag}(\alpha, \alpha^r, \ldots, \alpha^{r^{n-1}})$$

and let $\bar{B} = X^{-1}BX$.

Now if v is an element of the eigenspace V_α of $\bar{A}$ for the eigenvalue α, then

$$\bar{A}(\bar{B}v) = \bar{B}(\bar{B}^{-1}\bar{A}\bar{B})v = \bar{B}\bar{A}^r v = \alpha_i^r \bar{B}v$$

and the vector $\bar{B}v$ is an eigenvector of the matrix $\bar{A}$ for the eigenvalue α^r, thus $\bar{B}v \in V_{\alpha^r}$. Actually $\bar{B}$ defines an isomorphism between the 1-dimensional eigenspaces V_α and V_{α^r}. Note that $\bar{B}^n(v) \in V_\alpha$ and since V_α has dimension 1, $\bar{B}^n(v) = bv$ for some

$b \in F_p$. Let $v \in V_\alpha$ and $v \neq 0$. Thus $\{v\}$ is a basis for V_α and $\{v, \bar{B}(v), \dots \bar{B}^{n-1}(v)\}$ is a basis of $F_{p^e}^n$ for which $\bar{B}$ is of the form

$$\bar{B} = \begin{pmatrix} 0 & & & b \\ 1 & \ddots & & 0 \\ & \ddots & 0 & \vdots \\ & & 1 & 0 \end{pmatrix}.$$

The characteristic polynomial is $c_{\bar{B}} = x^n - b$, indeed $\bar{B} = C(x^n - b)$. In particular $b \in F_p$. Since $\bar{B}^n = bI_n$, we find the order of $\bar{B}$ as $t = n \operatorname{ord} b$ where $\operatorname{ord} b$ denotes the multiplictive order of $b \in F_p$. Theorem 3.17 states that any prime divisor of d, minimal such that $s|r^d - 1$, also divides t/d. Thus $n| \operatorname{ord} b$ and in particular $n|p-1$. □

Let $\Phi = \langle \varphi, \psi \rangle$ a fixed point free automorphism group on Z_p^n for arbitrary n and let each eigenvalue of φ over F_{p^e} have mulitplicity 1, e.g., $\operatorname{ord} \varphi | p^n - 1$ but $\operatorname{ord} \varphi \nmid p^l - 1$ for $l < n$. Then the proof of Proposition 5.25 holds and φ, psi are induced by matrices conjugate to block diagonal matrices $\bigoplus_{i=1}^m A_i, \bigoplus_{i=1}^m B_i$ where the A_i and B_i are of the same form as $\bar{A}$ and $\bar{B}$, respectively, in Proposition 5.25.

CHAPTER 6

The Abelian Case

Secondo Piatto: We are awaiting the fixed point free automorphism groups Φ of an abelian group G. By Proposition 3.3 and 1.15 it suffices to deal with the p-Sylow subgroups of G and to patch isomorphic fixed point free automorphism groups thereupon together.

Moreover, an abelian p-group G can be further decomposed, and we will show that its fixed point free automorphism groups can be constructed out of the fixed point free automorphism groups of elementary abelian groups. We use additive notation for abelian groups once again.

1. Transfer to the Elementary Abelian Case

We need the following theorem, which has important applications in representation theory also, to decompose an abelian p-group G into Φ-invariant direct factors. Even before this we have give some new definitions.

6.1. Definition. Let Φ be a group. A Φ-*module* G is an abelian group together with a scalar multiplication map

$$\cdot : \Phi \times G \to G$$

that satisfy the following axioms. Let $\varphi, \psi \in \Phi$ and $g, h \in G$.

(a) $\varphi(g+h) = \varphi g + \varphi h$.
(b) $(\varphi\psi)g = \varphi(\psi g)$.
(c) $1g = g$.

6.2. Definition. Let Φ be a group and let G, H be Φ-modules. A function $f : G \to H$ is an Φ-*module homomorphism* if for all $g_1, g_2 \in G$ and $\varphi \in \Phi$

(a) $f(g_1 + g_2) = f(g_1) + f(g_2)$,
(b) $f(\varphi m) = \varphi f(m)$.

6.3. Theorem (Maschke, Schur). Let Φ be a finite group of order k and G a Φ-module and let there be a Φ-endomorphism τ such that $\tau(kg) = g$ for all $g \in G$. Let $G = G_1 \oplus G_2^*$ be a direct decomposition of G as an abelian group such that G_1 is a Φ-submodule of G. Then there exists a direct decomposition $G = G_1 \oplus G_2$ as Φ-module.

Proof. see [**Hup67**], p.122. □

In our application, G will be an abelian p-group and Φ an automorphism group of order k where $k \nmid p$. The mapping $g \mapsto kg$ is an isomorphism with the inverse $\tau(g) = k^{-1}g$ and τ is a Φ-homomorphism. Thus the conditions for Theorem 6.3 are fulfilled. The assertion states that for every Φ-invariant direct factor G_1 of G there exists a Φ-invariant complement G_2 so $G = G_1 \oplus G_2$.

Theorem 6.3 gives the following

6.4. Lemma. Let G be an abelian p-group and Φ a group of automorphisms on G with $p \nmid |\Phi|$. Let p^d be the biggest invariant of G. Then G has a decomposition $G = G_1 \oplus G_2$, both G_1, G_2 are invariant under Φ, all abelian invariants of G_1 equal p^d and all the invariants of G_2 are smaller than p^d.

PROOF. Obviously, this is true for $d = 1$, i.e., G is elementary abelian. We carry out an induction on d with $\exp G = p^d$.

Suppose the assumption holds for all abelian p-groups G such that $\exp G = p^d$ and for all Φ on G such that $p \nmid |\Phi|$. For any abelian group G with $\exp G = p^{d+1}, d \geq 1$, and some Φ such that $p \nmid |\Phi|$, the group $F = pG$ has exponent p^d and is a characteristic subgroup of G. Thus the assumption holds for $F = F_1 \oplus F_2$.

Define

$$N = \{g \in G : pg \in F_2\}$$

which is Φ-invariant since F_2 is. It also has a Φ-invariant direct factor $\{g \in F_1 : pg = 0\}$. Theorem 6.3 guarantees the existence of a complement G_2 such that

$$N = \{g \in F_1 : pg = 0\} \oplus G_2$$

and G_2 is Φ-invariant. The abelian invariants of G_2 are at most $p \exp F_2 \leq p^d$, while the invariants of its complement in G are all equal to $p \exp F_1 = p^{d+1}$. Theorem 6.3 again implies there is a Φ-invariant factor $G_1 \leq G$ such that $G = G_1 \oplus G_2$. □

6.5. Proposition. Let G be an abelian p-group and Φ group of automorphisms on G with $p \nmid |\Phi|$. Then $G \cong \bigoplus_{i=1}^m G_i$, where $G_i = Z_{p^{d_i}}^{n_i}$ such that $d_1 > d_2 > \ldots > d_m$ and all G_i are Φ-invariant.

PROOF. By applying Lemma 6.4 iteratively. □

The previous Proposition 6.5 and Proposition 3.3 (a) enable us to split any fixed point free automorphism group Φ on an arbitrary abelian group G into isomorphic fixed point free automorphism groups Φ_i on factors G_i of G, with each G_i having only abelian invariants $p_i^{d_i}$ and $d_i \neq d_j$ for $p_i = p_j$.

Every fixed point free automorphism group Φ_i on

$$G_i \cong Z_{p_i^{d_i}}^{n_i}$$

induces a fixed point free automorphism group $\bar{\Phi}_i$ on the elementary abelian factor

$$G_i / p_i G_i \cong Z_{p_i}^{n_i}$$

and vice versa.

Now simply by determining the fixed point free automorphism groups $\bar{\Phi}_i$ on G_i/p_iG_i, extending them to Φ_i on G_i for all $i = 1, \ldots, m$ and finally patching those isomorphic Φ_i together via Proposition 3.3 (b), we find all fixed point free automorphism groups Φ on G.

The following Lemmata 6.6 to 6.8 state the connections between Φ on $G = Z_{p^d}^n$ and $\bar{\Phi}$ on G/pG more precisely.

6.6. Lemma. Let $G = Z_{p^d}^n$ and p prime. For $pG = \{pg : g \in G\}$ the factor group G/pG is isomorphic to Z_p^n. There is a natural epimorphism

$$\begin{aligned} h : \operatorname{Aut}(G) &\rightarrow \operatorname{Aut}(G/pG) \\ \alpha &\mapsto \bar{\alpha} \end{aligned}$$

with $\bar{\alpha} : x + pG \mapsto \alpha(x) + pG$ and

$$\operatorname{Ker} h = \{\alpha \in \operatorname{Aut}(G) : \forall g \in G \ \exists f \in pG : \alpha(g) = g + f\},$$

is a p-group.

Proof. The homomorphism h is well defined because pG is a characteristic subgroup of G.

Let $\{e_1, \dots, e_n\}$ denote a set of generators of G. If $\alpha \in \operatorname{Ker} h$, then for every e_i there is $f_i \in pG$ such that

$$\alpha(e_i) = e_i + f_i.$$

Every α defined in this way is an automorphism on G indeed and for each generator e_i we have $|pG| = p^{(d-1)n}$ possibilities to choose f_i from. Thus

$$|\operatorname{Ker} h| = \prod_{i=1}^{n} |pG| = p^{(d-1)n}.$$

Let $d > 1$ and $\bar{\alpha} \in \operatorname{Aut}(G/pG)$ such that

$$\bar{\alpha} : e_i + pG \mapsto \sum_{j=1}^{n} a_{ji} e_j + pG.$$

Then

$$\begin{array}{rcl} \alpha : G & \to & G \\ e_i & \mapsto & \displaystyle\sum_{j=1}^{n} a_{ji} e_j \end{array}$$

is linear on G. Suppose $\exists 0 \neq g \in G$ such that $\alpha(g) = 0$ in G. Obviously, $g \in pG$ since $\bar{\alpha}(g + pG) = 0 + pG$. Thus there is $f \in G$ such that $g = pf$. We denote f by g/p.

Now $\alpha(g/p) \in p^{d-1}G$, In particular, $\alpha(g/p) \in pG$ and $\bar{\alpha}(g/p + pG) = pG$. Again $g/p \in pG$ and there is $g/p^2 \in G$ with $g = p^2(g/p^2)$ and $\alpha(g/p^2) \in p^{d-2}G$.

By iteration downwards we get some $g/p^{d-1} \in G$ and $\alpha(g/p^{d-1}) \in pG$. Thus finally $g = p^d(g/p^d)$ for $g/p^d \in G$ and $g = 0$.

Hence α is an automorphism on G for which $h(\alpha) = \bar{\alpha}$ and h is an epimorphism indeed. □

Lemma 6.6 not only guarantees the existence of a pre-image α for any automorphism $\bar{\alpha} \in \operatorname{Aut}(G/pG)$ but its proof also gives a specific example of such an α.

6.7. Lemma. If $\Phi \leq \operatorname{Aut}(G)$ and $p \nmid |\Phi|$, then $h(\Phi)$ is isomorphic to Φ.

Conversely, if $\bar{\Phi} \leq \operatorname{Aut}(G/pG)$ and $p \nmid |\bar{\Phi}|$, then there is $\Phi \leq \operatorname{Aut}(G)$ such that $h(\Phi) = \bar{\Phi}$ and $h(\Phi)$ is isomorphic to $\bar{\Phi}$. Any two such groups Φ_1, Φ_2 are conjugate in $\operatorname{Aut}(G)$.

Proof. As $\operatorname{Ker} h$ is a p-group but $p \nmid |\Phi|$ we get $|h(\Phi)| = |\Phi|/|\Phi \cap \operatorname{Ker} h| = |\Phi|$ and $h(\Phi) \cong \Phi$.

On the other hand, since h is an epimorphism from $\operatorname{Aut}(G)$ to $\operatorname{Aut}(G/pG)$ there is a unique pre-image Φ^* with $h(\Phi^*) = \bar{\Phi}$ which includes $\operatorname{Ker} h$ for every subgroup $\bar{\Phi} \in \operatorname{Aut}(G/pG)$.

If additionally $p \nmid |\bar{\Phi}|$, then $[\Phi^* : \operatorname{Ker} h] = |\bar{\Phi}|$ and $|\operatorname{Ker} h| = p^{n(d-1)}$ are relatively prime and Theorem 1.33 assures that Φ^* contains subgroups of order $|\bar{\Phi}|$ and any two of them are conjugate in Φ^*.

Let Φ denote any of these complements of $\operatorname{Ker} h$. Then $h(\Phi) = \bar{\Phi}$ and Φ and $\bar{\Phi}$ are isomorphic. □

6.8. Lemma. If $\Phi \leq \operatorname{Aut}(G)$ is fixed point free on G, then $h(\Phi)$ is fixed point free on G/pG.

Conversely, if $\bar{\Phi} \leq \operatorname{Aut}(G/pG)$ is fixed point free on G/pG, then any $\Phi \leq \operatorname{Aut}(G)$ such that $h(\Phi) = \bar{\Phi}$ and $p \nmid |\Phi|$ is fixed point free on G.

Proof. Proposition 3.3 (c) shows that $h(\Phi)$ is fixed point free on G/pG.

Suppose $\Phi \leq \operatorname{Aut}(G)$ such that $h(\Phi) = \bar{\Phi}$ and $p \nmid |\Phi|$ but Φ is not fixed point free on G, i.e.,

$$\exists \operatorname{id}_G \neq \varphi \in \Phi \text{ and } \exists 0 \neq x \in G : \varphi(x) = x.$$

For $\bar{\varphi} := h(\varphi)$ we have $\bar{\varphi}(x + pG) = x + pG$ and since $\bar{\Phi}$ acts fixed point free on G/pG, we get $x \in pG$.

Let $g \in G \setminus pG$ such that $p^l g = x$ for some $l < d$. Thus $\varphi(g) \neq g$ and

$$p^l \varphi(g) = \varphi(p^l g) = \varphi(x) = x = p^l g.$$

Since $p^l(g - \varphi(g)) = 0$ and $l < d$ we have $g - \varphi(g) \in pG$ and $\varphi(g) = g + f$ with $f \in pG$. Then

$$\bar{\varphi}(g + pG) = \varphi(g) + pG = g + pG$$

and $\bar{\varphi} \neq \operatorname{id}_{G/pG}$ has a nontrivial fixed point, contrary to our assumption. □

The following proposition characterizes all fixed point free automorphism groups Φ on an abelian group G in terms of fixed point free automorphism groups on elementary abelian groups.

6.9. Proposition. Let G be an abelian group, $G \cong \bigoplus_{i=1}^m G_i$, where $G_i = Z^{n_i}_{p_i^{d_i}}$ and $d_i \neq d_j$ if $p_i = p_j$. The following are equivalent:

(a) The automorphism group Φ on G is fixed point free on G.
(b) The restriction $\Phi_i := \Phi|_{G_i}$ is isomorphic to Φ and fixed point free on G_i for every $i = 1, \ldots, m$.
(c) The order of Φ is not divisible by p_i and $\bar{\Phi}_i$ is fixed point free on $G_i/p_iG_i \cong Z^{n_i}_{p_i}$ for every $i = 1, \ldots, m$.

Proof.
$(a) \Rightarrow (b)$: Proposition 6.5 and Proposition 3.3 (a);
$(b) \Rightarrow (c)$: Proposition 3.3 (c);
$(c) \Rightarrow (a)$: Lemma 6.7, Lemma 6.8 and Proposition 3.3 (b). □

6.10. Corollary. Let G be an abelian group, $G \cong \bigoplus_{i=1}^m G_i$, where $G_i = Z^{n_i}_{p_i^{d_i}}$ and $d_i \neq d_j$ if $p_i = p_j$.

There is a fixed point free automorphism group Φ of size k if and only if $k|(p_i^{n_i} - 1)$ for all $1 \leq i \leq m$.

In particular, there is a cyclic fixed point free automorphism group of this size.

Proof. The necessary condition for a fixed point free automorphism group Φ follows directly from Proposition 6.9 (c) and Proposition 3.1.

Conversely, if $k|(p_i^{n_i}-1)$, then there is a cyclic fixed point free automorphism group $\langle\bar{\varphi}_i\rangle$ of order k on $Z_{p_i}^{n_i} \cong G_i/p_iG_i$ for every $i = 1, \ldots, m$ by Proposition 5.2. Lemma 6.7 and Lemma 6.8 state that there is a fixed point free automorphism group $\langle\varphi_i\rangle$ of order k on G_i and $\langle(\varphi_1, \ldots, \varphi_m)\rangle$ is fixed point free on G by Proposition 3.3 (b). □

Proposition 6.9 allows the computation of all fixed point free automorphism groups on an abelian group G. We just have to find isomorphic fixed point free automorphism groups $\bar{\Phi}_i$ on the elementary abelian groups G_i/p_iG_i and extend them onto G_i which is always possible by Lemma 6.7. Thus we get a bunch of conjugate possible extensions on G_i. We choose one Φ_i for each i and paste them together using automorphisms

$$a_i : \Phi_1 \to \Phi_i \text{ for } i > 1$$

to obtain

$$\Phi = \{(\phi_1, a_2(\phi_1), \ldots, a_m(\phi_1)) : \phi_1 \in \Phi_1\}$$

to be fixed point free on G via Proposition 3.3 (b).

Obviously, there is a variety of possibilities to choose Φ_i and a_i and lots of the resulting groups Φ will be conjugate in $\mathrm{Aut}(G)$, if not identical. The situation has to be clarified.

6.11. Proposition. Let G be an abelian group, $G \cong \bigoplus_{i=1}^m G_i$, where $G_i = Z_{p_i^{d_i}}^{n_i}$ and $d_i \neq d_j$ for $p_i = p_j$. Let Φ and Ψ be automorphism groups on G with p_i dividing the order of none of them for $i = 1, \ldots, m$. The following are equivalent:

(a) There is $x \in \mathrm{Aut}(G)$ such that
$$\Phi = x^{-1}\Psi x.$$

(b) There is $x \in \mathrm{Aut}(G)$ with $x(G_i) = G_i$ for $i = 1, \ldots, m$ such that
$$\bar{\Phi} = \bar{x}^{-1}\bar{\Psi}\bar{x}$$
in $G/F(G)$.

Proof.

$(a) \Rightarrow (b)$: Let $G = \bigoplus_{i=1}^d S_{p_i}$ be the factorization of G into its p-Sylow subgroups S_{p_i} for $1 \leq i \leq d$. Since $\mathrm{Aut}(G) \cong \bigoplus_{i=1}^d \mathrm{Aut}(S_{p_i})$ we can, w.l.o.g., assume G is a p-group and $d_1 > d_2 > \ldots > d_m$.

If $\Phi = x^{-1}\Psi x$ in $\mathrm{Aut}(G)$, then $\bar{\Phi} = \bar{x}^{-1}\bar{\Psi}\bar{x}$ in $\mathrm{Aut}(G/pG)$. All we have to do is to construct an automorphism x^* which transfers Ψ into Φ but leaves G_i invariant for all $i = 1, \ldots, m$.

Let φ, ψ be fixed such that $\bar{\varphi} = \bar{x}^{-1}\bar{\psi}\bar{x}$. Since φ, ψ both leave G_i invariant for $i = 1, \ldots, m$, we have $\bar{\varphi} : v \mapsto Av, \bar{\psi} : v \mapsto Bv$ with $v \in G/pG$ and

$$\begin{aligned} A &= A_{11} \oplus \ldots \oplus A_{mm}, \\ B &= B_{11} \oplus \ldots \oplus B_{mm} \end{aligned}$$

with $A_{ii}, B_{ii} \in \mathrm{Aut}(G_i/pG_i)$. Note that we regard the elementary abelian group G/pG as n-dimensional vector space and represent the automorphisms as matrices in $GL(n,p)$, with $n = n_1 + \cdots + n_m$ again.

Since x is an arbitrary automorphism, the matrix X with $\bar{x} : v \mapsto Xv$ is not of block diagonal form in general. For all $g \in G_i$, the order $\operatorname{ord}(g) \leq p^{d_i}$ and also $\operatorname{ord}(x(g)) = \operatorname{ord}(g) \leq p^{d_i}$. Thus, for $x \in \operatorname{Aut}(G)$ we obtain

$$x(g) \in \bigoplus_{j=1}^{i-1} pG_i \oplus \bigoplus_{j=i}^{m} G_i$$

and

$$\bar{x}(g + pG) = x(g) + pG \in \bigoplus_{j=i}^{m} G_i/pG_i.$$

In general, $\bar{x} : v \mapsto Xv$ and

$$X = \begin{pmatrix} X_{11} & \cdots & X_{1m} \\ & \ddots & \vdots \\ 0 & & X_{mm} \end{pmatrix}$$

with $X_{ij} \in \operatorname{Hom}(G_i/pG_i, G_j/pG_j)$. Let $\bar{x}^{-1} : v \mapsto Yv$ with $Y = X^{-1}$ of the same upper triangular form

$$Y = \begin{pmatrix} Y_{11} & \cdots & Y_{1m} \\ & \ddots & \vdots \\ 0 & & Y_{mm} \end{pmatrix}.$$

Now

$$XY = (XY)_{ij} = (\sum_{k=1}^{m} X_{ik}Y_{kj})_{ij} = (\sum_{k=j}^{i} X_{ik}Y_{kj})_{ij} = I$$

the identity mapping on G/pG. In particular, for $i = j$ we have $(XY)_{ii} = X_{ii}Y_{ii} = I_{n_i}$, the identity on G_i/pG_i, and $Y_{ii} = X_{ii}^{-1}$ the unique inverse which exists since X_{ii} has full rank. The equation $\bar{\varphi} = \bar{x}^{-1}\bar{\psi}\bar{x}$ now becomes:

$$\begin{aligned} A &= X^{-1}BX \\ &= \begin{pmatrix} X_{11}^{-1} & \cdots & Y_{1m} \\ & \ddots & \vdots \\ 0 & & X_{mm}^{-1} \end{pmatrix} \begin{pmatrix} B_{11} & \cdots & 0 \\ & \ddots & \vdots \\ 0 & & B_{mm} \end{pmatrix} \begin{pmatrix} X_{11} & \cdots & X_{1m} \\ & \ddots & \vdots \\ 0 & & X_{mm} \end{pmatrix} \\ &= \begin{pmatrix} X_{11}^{-1} & \cdots & Y_{1m} \\ & \ddots & \vdots \\ 0 & & X_{m,m}^{-1} \end{pmatrix} \begin{pmatrix} B_{1,1}X_{11} & \cdots & \sum_{k=1}^{m} B_{kk}X_{km} \\ & \ddots & \vdots \\ 0 & & B_{m,m}X_{mm} \end{pmatrix} \\ &= \begin{pmatrix} X_{11}^{-1}B_{1,1}X_{11} & & 0 \\ & \ddots & \\ 0 & & X_{mm}^{-1}B_{m,m}X_{mm} \end{pmatrix} \end{aligned}$$

Note that the last equality is forced since A on the left side is of diagonal form. For each i there is $X_{ii} \in \operatorname{Aut}(G_i/pG_i)$ such that

$$A_{ii} = X_{ii}^{-1}B_{ii}X_{ii}.$$

By Lemma 6.6 there is an automorphism x_i on G_i such that

$$\bar{x^*}_i : v \mapsto X_{ii}v$$

on G_i/pG_i. Let $\bar{\Phi}_i = \bar{\Phi}|_{G_i/pG_i}$ and $\bar{\Psi}_i = \bar{\Psi}|_{G_i/pG_i}$. Then $\bar{\Phi}_i = \bar{x^*}_i^{-1}\bar{\Psi}_i\bar{x}_i^*$ and by Lemma 6.7 any two extensions Φ_i of $\bar{\Phi}_i$ on G_i are conjugate in $\operatorname{Aut}(G_i)$ for $i = 1, \dots, m$. The same holds for extensions Ψ_i on G_i. W.l.o.g., we assume

$$\Phi_i = (x_i^*)^{-1}\Psi_i x_i^*.$$

Then $\Phi = (x^*)^{-1}\Psi x^*$ for $x^* \in \operatorname{Aut}(G)$ with $x^*|_{G_i} = x_i^*$.

$2 \Rightarrow 1$: Let

$$\begin{array}{rcl} h : \operatorname{Aut}(G) & \to & \operatorname{Aut}(G/F(G)) \\ \alpha & \mapsto & \bar{\alpha} \end{array}$$

with $\bar{\alpha} : g + F(G) \mapsto \alpha(g) + F(G)$.

For all groups $\Phi, \Psi \leq \operatorname{Aut}(G)$ such that $h(\Phi) = \bar{\Phi}$ and $h(\Psi) = \bar{\Psi}$ there is some $x \in \operatorname{Aut}(G)$ such that $h(\Phi) = h(x)^{-1}h(\Psi)h(x)$. Thus the pre-image of $h(\Phi)$ is

$$\langle \Phi, \operatorname{Ker} h \rangle = \langle x^{-1}\Psi x, \operatorname{Ker} h \rangle =: H.$$

Now

$$\operatorname{Ker} h = \{\alpha \in \operatorname{Aut}(G) : \forall g \in G, \exists f \in F(G) : \alpha(g) = g + f\}$$

is isomorphic to the direct product of automorphism groups on the Sylow subgroups of G. For determining the order of $\operatorname{Ker} h$, we compute the number of automorphisms of the form $g \mapsto g + F(G)$ on each Sylow subgroup and multiply them up.

To simplify notation we assume $G \cong \bigoplus_{i=1}^m G_i$ to be a p-group. Let $\{e_{i1}, \dots, e_{in_i}\}$ be a set of generators of G_i for $i = 1, \dots, m$. If $\alpha \in \operatorname{Ker} h$, then for every e_{ij} there is $f_{ij} \in F(G) = pG$ and $\operatorname{ord} f_{ij} \leq \operatorname{ord} e_{ij}$ such that

$$\alpha(e_{ij}) = e_{ij} + f_{ij}.$$

Every α defined in this way is an automorphism on G indeed. For each generator e_{ij} we can choose f_{ij} from $pG \cap G_{p^{d_i}}$, where $G_{p^{d_i}} = \{x \in G : p^{d_i}x = 0\}$. Now

$$|\operatorname{Ker} h| = \prod_{i=1}^m |pG \cap G_{p^{d_i}}|^{n_i}$$

and $\operatorname{Ker} h$ is a p-group.

Thus for arbitrary abelian G we have $\operatorname{Ker} h$ to be a direct product of p_i-groups, where p_i are the prime divisors of $|G|$.

Since $|\operatorname{Ker} h|$ and $[H : \operatorname{Ker} h] = |\bar{\Phi}|$ are relatively prime, Theorem 1.33 assures that H contains subgroups of order $|\bar{\Phi}|$ and any two of them are conjugate in H. Let Φ denote any of these complements of $\operatorname{Ker} h$. Then $h(\Phi) = \bar{\Phi}$ and they are isomorphic.

In the same way we choose Ψ as some complement of $\operatorname{Ker} h$ in xHx^{-1}, then Φ and Ψ are conjugate in $\operatorname{Aut}(G)$. □

Proposition 6.11 gives a one to one correspondence between non conjugate fixed point free automorphism groups on

$$G = \bigoplus_{i=1}^m Z_{p_i^{d_i}}^{n_i}$$

and the isomorphic fixed point free automorphism groups on

$$\bigoplus_{i=1}^m Z_{p_i}^{n_i}$$

in $\bigoplus_{i=1}^{m} \mathrm{Aut}(Z_{p_i}^{n_i})$ which are non conjugate therein. This enables us to transfer all our knowledge on elementary abelian groups to arbitrary abelian groups G.

2. Cyclic Φ

Once again, first we concentrate on Φ to be cyclic. Although the form of an automorphism φ on G generating a fixed point free automorphism group is clear by Proposition 6.9, we state it explicitly.

6.12. Corollary. Let G be an abelian group, $G = \bigoplus_{i=1}^{m} G_i$, where $G_i \cong Z_{p_i^{d_i}}^{n_i}$ and $d_i \neq d_j$ if $p_i = p_j$. The automorphism $\varphi \in \mathrm{Aut}(G)$ generates a fixed point free automorphism group of order k on G if and only if

$$\varphi = (\varphi_1, \dots, \varphi_m),$$

where $\langle \varphi_i \rangle$ is a fixed point free automorphism group of order k on G_i for $i = 1, \dots, m$.

Proof. This is a reformulation of Proposition 6.9 for cyclic groups Φ. □

Another specialization:

6.13. Corollary. Let $\varphi, \psi \in \mathrm{Aut}(G)$ both generate a fixed point free automorphism group of order k on G.

$$\langle \varphi \rangle \simeq \langle \psi \rangle \text{ in } \mathrm{Aut}(G) \;\Leftrightarrow\; \langle \bar{\varphi} \rangle \simeq \langle \bar{\psi} \rangle \text{ in } \bigoplus_{i=1}^{m} \mathrm{Aut}(G_i/p_iG_i).$$

Proof. This is a reformulation of Proposition 6.11 for cyclic groups Φ. □

In the following let G always denote the abelian group,

$$G = \bigoplus_{i=1}^{m} G_i,$$

where $G_i \cong Z_{p_i^{d_i}}^{n_i}$ and $d_i \neq d_j$ if $p_i = p_j$. We obtain the number of non conjugate cyclic fixed point free automorphism groups on G by building up the same structures as in the elementary abelian case. The only change necessary is to think in $i = 1, \dots, m$ in parallel.

6.14. Definition. For a fixed k let R denote the set of m-tuples $\varphi = (\varphi_1, \dots, \varphi_m)$ of rational canonical forms for automorphisms φ_i, which generate a fixed point free automorphism group of order k on $Z_{p_i}^{n_i} \cong G_i/p_iG_i$, i.e., R is a set of representatives for each conjugacy class of automorphisms in $\bigoplus_{i=1}^{m} \mathrm{Aut}(Z_{p_i}^{n_i})$ generating a fixed point free automorphism group of order k on $\bigoplus_{i=1}^{m} G_i$.

For an arbitrary subgroup $U \leq Z_k^*$, let

$$R_U = \{\varphi \in R : \varphi^r \simeq \varphi, \forall r \in U\}.$$

Let

$$E_i = \langle p_i \rangle = \{1, p_i, \dots, p_i^{e_i - 1}\} \leq Z_k^*,$$

where e_i is the smallest natural number such that $k | (p_i^{e_i} - 1)$ and

$$E = \bigcap_{i=1}^{m} E_i.$$

Then

$$R_E = R.$$

6.15. Lemma. Let $\varphi = (\varphi_1, \dots, \varphi_m) \in R$.

$$\varphi \in R_U \quad \Leftrightarrow \quad \forall r \in U, \forall i = 1, \dots, m : \varphi_i^r \simeq \varphi_i.$$

Proof. trivial. □

Now we are using this characterization for counting the elements of R_U.

6.16. Lemma. Let $t_i = |\langle E_i, U\rangle|$ for $1 \leq i \leq m$.

$$|R_U| = \begin{cases} \prod_{i=1}^m \begin{pmatrix} \frac{\phi(k)}{t_i} + \frac{n_i}{t_i} - 1 \\ \frac{n_i}{t_i} \end{pmatrix} & \text{if } t_i | n_i \text{ for all } i \\ 0 & \text{else} \end{cases}$$

Proof. By Lemma 6.15 we only have to build all m-tuples φ, where $\varphi_i^r \simeq \varphi_i$ for $r \in U$ for all $i = 1, \dots, m$. These φ_i and their numbers are determined by Lemma 5.6 and 5.9. By multiplying them up we get the above expression. □

What is more, we get exactly the same formula for the number of non conjugated cyclic fixed point free automorphism groups of order k on G abelian as on Z_p^n.

6.17. Proposition. Let $\mathcal{U} = \{U \leq Z_k^* : E \leq U\}$. There are exactly

$$\mathcal{N}_k = \frac{1}{\phi(k)} \sum_{U \in \mathcal{U}} |U|(|R_U| - |\bigcup_{W>U} R_W|)$$

non conjugate cyclic fixed point free automorphism groups of order k on G, abelian.

Proof. The same argumentation as used for the elementary abelian case (Proposition 5.12) gives the above expression for non conjugate fixed point free automorphism groups of order k in $\bigoplus_{i=1}^m \mathrm{Aut}(G_i/p_iG_i)$, which equals the number of non conjugated fixed point free automorphism groups of order k on $G = \bigoplus_{i=1}^m G_i$ by Corollary 6.13. □

The evaluation of $|\bigcup_{W \in \mathcal{U}, W>U} R_W|$ has still to be done. Evidently, it suffices to do the union over all minimal groups $W > U$, that is over all groups W such that $[W : U]$ is prime. In general, we have:

6.18. Proposition. Let $\mathcal{W} = \{W \leq Z_k^* \ : \ [W : U] \text{ prime}, |R_W| \neq 0\}$. Then

$$\begin{aligned} |\bigcup_{W \in \mathcal{U}, W>U} R_W| &= |\bigcup_{W \in \mathcal{W}} R_W| \\ &= \sum_{j=1}^{|\mathcal{W}|} (-1)^{j-1} \sum_{W_1, \dots, W_j \in \mathcal{W}, \text{pairwise distinct}} |R_{\langle \bigcup_{h=1}^j W_h \rangle}| \end{aligned}$$

Proof. Since for $U < W_1 \leq W_2$ the set R_{W_2} is a subset of R_{W_1}, the first equality holds. The second follows from standard inclusion-exclusion counting of the elements of a union of non-disjoint sets. □

By Lemma 6.16 we have $|R_{\langle \bigcup_{h=1}^j W_h \rangle}| = 0$ if the order of $\langle E_i, \bigcup_{h=1}^j W_h \rangle$ does not divide n_i for every $i = 1, \dots, m$. Thus lots of summands will vanish in the above formula.

6.19. Lemma. Let $u = \gcd(n_1, \dots, n_m, \phi(k))$. If $|W| > u$ then $|R_W| = 0$.

PROOF. This can be seen immediately from Lemma 6.16. □

We look at some particularly well behaved specializations

6.20. Corollary. If $u = |E|$, then

$$\mathcal{N}_k = \frac{|E|}{\phi(k)}|R|.$$

6.21. Corollary. If $u/|E|$ is prime, then

$$\mathcal{N}_k = \frac{|E|}{\phi(k)}\big[|R| + (\frac{u}{|E|} - 1) \sum_{|W| \in \mathcal{U}, |W| = u} |R_W|\big].$$

6.22. Corollary. For k equal to 4 or an odd prime power or 2 times an odd prime power, Z_k^* is cyclic, i.e., the subgroup lattice of Z_k^* is linearly ordered: for some l

$$E = U_0 < U_1 < \dots < U_l = Z_k^*$$

with $[U_{i+1} : U_i]$ prime and

$$N_k = \frac{1}{\phi(k)} \sum_{i=0}^{l} |U_i|(|R_{U_i}| - |R_{U_{i+1}}|),$$

where $|R_{U_{l+1}}| = 0$ for ease of notation.

Note that the counting arguments given above can also be transferred to groups with nonabelian p_i-Sylow subgroups G_i but we fail to give a formula for $|R_U|$ in this case.

6.23. Example. We would like to compute the number of non conjugate fixed point free automorphism groups of order 8 on the group $G = Z_5^4 \times Z_{49}^2$. Evidently, this is equal to the number for $Z_5^4 \times Z_7^2$ or in general for $Z_{5^i}^4 \times Z_{7^j}^2$ with some integers i, j.

8 divides $5^2 - 1$ and $7^2 - 1$. Thus $E_1 = \{1, 5\} \leq Z_8^*$ and $E_2 = \{1, 7\} \leq Z_8^*$; the intersection is $E = E_1 \cap E_2 = \{1\}$ and $\langle E_1, E_2 \rangle = Z_8^*$. Since $u = \gcd(4, 2, \phi(8)) = 2$, we can actually use Corollary 6.21. We compute

$$R_{\langle 1 \rangle} = \binom{4/2 + 4/2 - 1}{4/2}\binom{4/2 + 2/2 - 1}{2/2} = 3 \cdot 2 = 6,$$

$$R_{E_1} = 0,$$

$$R_{E_2} = \binom{4/4 + 4/4 - 1}{4/4}\binom{4/2 + 2/2 - 1}{2/2} = 1 \cdot 2 = 2,$$

$$R_{Z_8^*} = 0$$

via Lemma 6.16 and obtain

$$\mathcal{N}_8 = \frac{1}{4}\big[6 + (\frac{2}{1} - 1)(0 + 2)\big] = 2$$

which actually equals the number of non conjugate fixed point free automorphism groups of order 8 on the group Z_5^4 (see the example in chapter 5).

3. Quaternion Φ

We are working ourselves up to quaternion fixed point free automorphism groups on G although we do not give their explicit form in general as done for the elementary abelian case. Recall that being abelian is a necessary condition on a group G to admit a fixed point free automorphism of order 2. Thus the following proposition is the definitive existence result.

6.24. Proposition. Let G be an abelian group, $G = \bigoplus_{i=1}^m G_i$, where $G_i \cong Z_{p_i^{d_i}}^{n_i}$ and $d_i \neq d_j$ if $p_i = p_j$. There exists a quaternion fixed point free automorphism group of order 2^{t+1} on G if and only if for every $i = 1, \ldots, m$ it holds $2^{t+1} | p_i^{n_i} - 1$ and either $2|n_i$ and $2^t | p_i + 1$ or $2e_i | n_i$, where e_i is the smallest natural number such that $2^t | p_i^{e_i} - 1$.

Proof. Proposition 6.9, 5.17 and 5.19 together give the result. □

For the simple case $2^{t+1} = 8$ we can also state

6.25. Corollary. There exists a quaternion fixed point free automorphism group Φ of order 8 on G if and only if for every $i = 1, \ldots, m$ it holds $2 \nmid p_i$ and $2|n_i$. Any such Φ is conjugated to the group $\langle \varphi, \psi \rangle$ with $\varphi_i = \varphi|_{G_i} : v \mapsto A_i v$ and $\psi_i = \psi|_{G_i} : v \mapsto B_i v$ where

$$A_i = \bigoplus_{j=1}^{n_i/2} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, B_i = \bigoplus_{j=1}^{n_i/2} \begin{pmatrix} u_i & v_i \\ v_i & -u_i \end{pmatrix},$$

and $u_i^2 + v_i^2 + 1 = 0 \bmod p_i^{d_i}$.

Proof. Proposition 6.24 gives the sufficient and necessary conditions on G. It is easy to see that $\langle \varphi, \psi \rangle$ as given in the hypothesis exists and is fixed point free on G. Corollary 5.20 shows all groups Φ to be conjugate. □

6.26. Corollary. Let G of order p^n, n odd. Then all fixed point free automorphism groups on G are of type (I).

Proof. For abelian $G = \bigoplus_{i=1}^m G_i$, where $G_i \cong Z_{p^{d_i}}^{n_i}$ the sum $\sum_{i=1}^m d_i n_i = n$ is odd, thus there is some n_i odd, and G has no quaternion fixed point free automorphism group by Proposition 6.24 □

6.27. Proposition. Let $\mathcal{U} = \{U \leq Z_k^* : \langle E, -1 \rangle \leq U\}$ and let R_U denote the set of representatives for each conjugacy class of automorphisms in $\bigoplus_{i=1}^m \mathrm{Aut}(Z_{p_i}^{n_i})$ generating a fixed point free automorphism group of order $k = 2^t$ on $\bigoplus_{i=1}^m Z_{p_i}^{n_i}$ such that $\varphi^r \simeq \varphi$ for all $r \in U$. Then there are exactly

$$\frac{1}{2^{t-1}} \sum_{U \in \mathcal{U}} |U| (|R_U| - | \bigcup_{W > U} R_W|)$$

non conjugate quaternion fixed point free automorphism groups of order $2^t + 1$ on $G = \bigoplus_{i=1}^m Z_{p_i^{d_i}}^{n_i}$ with $d_i \neq d_j$ for $p_i = p_j$.

Proof. This follows from Proposition 5.20 and Corollary 6.13. □

4. Φ of type (I)

Similarly, we can also generalize our results on Φ with cyclic Sylow subgroups on elementary abelian groups G.

6.28. Lemma. Let G be an abelian group, $G = \bigoplus_{i=1}^{m} G_i$, where $G_i \cong Z_{p_i^{d_i}}^{n_i}$ and $d_i \neq d_j$ for $p_i = p_j$. Let Φ be a non cyclic fixed point free automorphism group on G with cyclic Sylow subgroups, i.e., $\Phi = \langle \varphi, \psi \rangle$ where $\varphi^s = \psi^t = \mathrm{id}, \psi^{-1}\varphi\psi = \varphi^r$ and $r^t \equiv 1(s), \gcd(s, t(r-1)) = 1$ and $|\Phi| = st$.

Let d be the smallest natural number such that $s | r^d - 1$. Then d divides $\gcd(n_1, \dots, n_m, \phi(s), t)$ and $d > 1$.

Proof. By Lemma 5.23 and Proposition 6.9. □

6.29. Corollary. Let G be an abelian group, $G = \bigoplus_{i=1}^{m} G_i$, where $G_i \cong Z_{p_i^{d_i}}^{n_i}$ and $d_i \neq d_j$ for $p_i = p_j$. If

$$\gcd(n_1, \dots, n_m, p_1^{n_1} - 1, \dots, p_m^{n_m} - 1) = 1,$$

then every fixed point free automorphism group Φ on G is cyclic.

Proof. Same as the corresponding proof for G elementary abelian, Corollary 5.24. □

We give one more statement on arbitrary p-groups.

6.30. Proposition. Let G be of order p^n, p, n prime, and not elementary abelian. Then each fixed point free automorphism group Φ on G is cyclic and its order is a divisor of $p - 1$.

Proof. By Proposition 3.3 a necessary condition on G for having a fixed point free automorphism group Φ is the existence of isomorphic fixed point free automorphism groups on $F(G)$ and $G/F(G)$, which are both non trivial since G is not elementary abelian. Let $|F(G)| = p^s$ and $|G/F(G)| = p^t$ with $s+t = n$. Obviously, the order k of Φ has to divide

$$\gcd(p^s - 1, p^t - 1) = p^{\gcd(s,t)} - 1.$$

Since $s + t = n$ prime, thus $\gcd(s, t) = 1$, the size k is bounded by $p - 1$.

W.l.o.g., $F(G)$ is elementary abelian; $F^{(i)}(G)$ is for some i. Suppose there is a non cyclic, fixed point free automorphism group Φ on G. According to Lemma 5.23 there is an integer $m > 1$ such that $m|s$ and $m|t$, but $\gcd(s, t) = 1$.

So G admits only cyclic fixed point free automorphism groups. □

Note that by Proposition 3.3 it suffices that an arbitrary group G has a characteristic subgroup or factor group of order p^n, with primes p and n, which is not elementary abelian, and G admits only cyclic fixed point free automorphism groups of an order dividing $p - 1$.

CHAPTER 7

Applications of Fixed Point Free Automorphism Groups

Satisfied by the last 3 dishes we have a little something in between: examples for structures wherein fixed point free automorphism groups arise quite naturally. In particular, we show their connections with Frobenius groups, planar nearrings and nearfields.

1. Frobenius Groups

We cite the famous criterion for the non-simplicity of a group by Wielandt to provide the background for our introduction of Frobenius groups, but make no further use of it. For the proof, which extensively relies on character theory, we refer to [**Rob96**].

7.1. Theorem (Wielandt). Let G be a finite group with subgroups H and K such that $K \lhd H$ and $H \cap H^x \leq K$ for all $x \in G \setminus H$. Let N be the set of elements of G which do not belong to any conjugate of $H \setminus K$. Then N is a normal subgroup of G such that $G = HN$ and $H \cap N = K$.

Proof. see [**Rob96**], p.248. □

Frobenius obtained this result for the case $K = \{1_G\}$, thus describing groups which are of special interest.

7.2. Definition. A group G is called *Frobenius group* if it has a proper non trivial subgroup $H < G$ such that $H \cap H^g = \{1_G\}$ for all $g \in G \setminus H$.

$N = G \setminus \bigcup_{g \in G} (H \setminus \{1_G\})^g$ is a normal subgroup of G such that $G = HN$ and $H \cap N = \{1_G\}$, i.e., G is a semidirect product of H and N. We call N the *Frobenius kernel* and H a *Frobenius complement*.

By the following proposition we find that a finite Frobenius group with kernel N and complement H and a group with fixed point free automorphism group are essentially the same.

7.3. Proposition ([Hup67](V. 8.5)).

(a) Let G be a Frobenius group with complement H and kernel N then the mapping $\tau : H \to \mathrm{Aut}(N), h \mapsto \varphi_h$ where $\varphi_h(n) = hnh^{-1}$ for $h \in H, n \in N$ is an isomorphism from H to a fixed point free automorphism group $\Phi := \tau(H)$ on N.

(b) Let Φ be a fixed point free automorphism group on the additive group $(N, +)$. Then the semidirect product $G = \Phi \ltimes N$ with the group operation

$$(\varphi_1, n_1)(\varphi_2, n_2) = (\varphi_1\varphi_2, \varphi_2(n_1) + n_2)$$

is a Frobenius group with complement $\Phi \ltimes \langle 0_N \rangle$ and kernel $\langle \mathrm{id}_N \rangle \ltimes N$.

PROOF.

(a) Let $h_1, h_2 \in H$. Then $\tau(h_1h_2) = \varphi_{h_1h_2}$ and
$$\varphi_{h_1h_2} : n \mapsto h_1h_2nh_2^{-1}h_1^{-1}$$
whereas $\tau(h_1)\tau(h_2) = \varphi_{h_1}\varphi_{h_2}$ and
$$\varphi_{h_1}\varphi_{h_2} : n \mapsto h_1h_2nh_2^{-1}h_1^{-1}.$$
So τ is a homomorphism. Suppose there are $h \in H$ and $n \in N$ such that $\varphi_h(n) = hnh^{-1} = n$, then
$$n^{-1}hn = h \in H \cap H^n.$$
Either $h = 1_G$ and $\phi_h = \mathrm{id}_N$ or $n = 1_G$ by the definition of a Frobenius group. Thus τ is an isomorphism and $\tau(H)$ is a fixed point free automorphism group on N.

(b) It is easy to see that $G = \Phi \ltimes N$ with the multiplication defined as above is a group indeed. Let $H = \Phi \ltimes \langle 0_N \rangle$ and $g = (\varphi_g, n_g) \in G \setminus H$. Suppose $h = (\varphi_h, 0_N) \in H \cap H^g$. Then there is $x = (\varphi_x, 0_N) \in H$ such that
$$\begin{aligned} h &= g^{-1}xg \\ &= (\varphi_g^{-1}, -\varphi_g^{-1}(n_g))(\varphi_x, 0_N)(\varphi_g, n_g) \\ &= (\varphi_g^{-1}, -\varphi_g^{-1}(n_g))(\varphi_x\varphi_g, \varphi_g(0_N) + n_g) \\ &= (\varphi_g^{-1}, -\varphi_g^{-1}(n_g))(\varphi_x\varphi_g, n_g) \\ &= (\varphi_g^{-1}\varphi_x\varphi_g, \varphi_x\varphi_g\varphi_g^{-1}(-n_g) + n_g) \\ &= (\varphi_g^{-1}\varphi_x\varphi_g, -\varphi_x(n_g) + n_g). \end{aligned}$$
Thus $\varphi_h = \varphi_g^{-1}\varphi_x\varphi_g$ and $0_N = -\varphi_x(n_g) + n_g$ resulting in $\varphi_x = \mathrm{id}_N = \varphi_h$ and $h = (\mathrm{id}_N, 0_N)$. Hence $H \cap H^g = \{(\mathrm{id}_N, 0_N)\}$ for each $g \in G \setminus H$ and G is a Frobenius group with complement $\Phi \ltimes \langle 0_N \rangle$ and kernel $\langle \mathrm{id}_N \rangle \ltimes N$.

□

The objective of this paper is to provide means for the construction of fixed point free automorphism groups Φ on a group N, thus in terms of Frobenius groups speaking, we start with a kernel N and determine feasible complements H such that the semidirect product HN is a Frobenius group.

We mention one more interesting connection between automorphism groups Φ on N and semidirect products $\Phi \ltimes N$.

7.4. Proposition. Let Φ, Ψ be fixed point free automorphism groups on the group $(N, +)$. The following are equivalent:

(a) $\Phi \ltimes N$ and $\Psi \ltimes N$ are isomorphic.

(b) Φ and Ψ are conjugate in $\mathrm{Aut}(N)$.

PROOF. $(a) \Rightarrow (b)$: By Proposition 7.3 both $\Phi \ltimes N$ and $\Psi \ltimes N$ are Frobenius groups with kernel N and complement Φ and Ψ, respectively. Since the kernel of a Frobenius group is unique and the complement is unique up to conjugacy by Theorem 1.33 any isomorphism
$$i : \Phi \ltimes N \to \Psi \ltimes N$$
is of the form
$$i : (\varphi, n) \mapsto (a(\varphi), b(n))$$

where $a : \Phi \to \Psi$ is an isomorphism and $b \in \mathrm{Aut}(N)$.

For all $\varphi_1, \varphi_2 \in \Phi$ and for all $n_1, n_2 \in N$ we need $i((\varphi_1, n_1)(\varphi_2, n_2)) = i((\varphi_1, n_1))i((\varphi_2, n_2))$.

$$i((\varphi_1, n_1)(\varphi_2, n_2)) = (a(\varphi_1\varphi_2), b(\varphi_2(n_1) + n_2))$$

and

$$\begin{aligned} i((\varphi_1, n_1))i((\varphi_2, n_2)) &= (a(\varphi_1), b(n_1))(a(\varphi_2), b(n_2)) \\ &= (a(\varphi_1)a(\varphi_2), a(\varphi_2)(b(n_1)) + b(n_2)). \end{aligned}$$

Thus

$$a(\varphi_1\varphi_2) = a(\varphi_1)a(\varphi_2),$$

that is, a is an homomorphism from Φ to Ψ, and

$$\begin{aligned} b(\varphi_2(n_1) + n_2) &= (a(\varphi_2)b)(n_1) + b(n_2) \\ \varphi_2(n_1) + n_2 &= (b^{-1}a(\varphi_2)b)(n_1) + n_2, \end{aligned}$$

that is, $\varphi_2 = b^{-1}a(\varphi_2)b$ for every $\varphi_2 \in \Phi$ thus $a : \varphi \mapsto b\varphi b^{-1}$ and $b\Phi b^{-1} = \Psi$ for $b \in \mathrm{Aut}(N)$.

$(b) \Rightarrow (a)$: Let $\Phi = b^{-1}\Psi b$ for $b \in \mathrm{Aut}(N)$ and define a homomorphism

$$\begin{aligned} i : \Phi \ltimes N &\to \Psi \ltimes N \\ (\varphi, n) &\mapsto (b\varphi b^{-1}, b(n)). \end{aligned}$$

It is easy to see that i is an isomorphism. □

Thus if we want to find all non isomorphic Frobenius groups with a given kernel N, we can restrict our search on all non conjugate fixed point free automorphism groups on N.

2. Planar Nearrings

Another structure which heavily relies on regular automorphism groups on some group, as has been shown by Ferrero, are planar nearrings. We follow the development of Clay in [**Cla92**] where we can also find a survey of applications of planar nearrings in design theory.

7.5. Definition. A *nearring* $(N, +, \cdot)$ is a set with two operations $+$ and $\cdot$ such that

(a) $(N, +)$ is a group;
(b) $(N \setminus \{0\}, \cdot)$ is a semigroup;
(c) $(n_1 + n_2) \cdot n_3 = n_1 \cdot n_3 + n_2 \cdot n_3$ for all $n_1, n_2, n_3 \in N$.

To be precise, by requiring the right distributive law we obtained right nearrings. Of course, left nearrings are defined with the appropriate modifications and their respective theory corresponds by simply rewriting the multiplication order.

7.6. Definition. Let $(N, +, \cdot)$ be a nearring. For $a, b \in N$ we define a relation:

$$a \equiv b \Leftrightarrow a \cdot x = b \cdot x \text{ for all } x \in N$$

If $a \equiv b$, then a and b are called *equivalent multipliers.*

It is easy to see that $\equiv$ is a equivalence relation indeed.

7.7. Definition. A nearring $(N, +, \cdot)$ is called *planar*, if the following conditions hold:

(a) $\equiv$ induces at least 3 equivalence classes, $|N/\equiv| \geq 3$.
(b) The equation

$$x \cdot a = x \cdot b + c$$

has a unique solution for any $a, b, c \in N, a \not\equiv b$.

We present a method for constructing finite planar nearrings which is due to Giovanni Ferrero.

7.8. Definition. Let $(N, +)$ be a finite additive group and Φ a fixed point free automorphism group on N. We choose some of the nontrivial orbits, say m ones, and for each of them we fix a representative $e_i, 1 \leq i \leq m$.

$$N^* = \bigcup_{i=1}^{m} \Phi(e_i)$$

be the union of these orbits $\Phi(e_i)$. Then we can define a multiplication "$\cdot$" on N by

$$x \cdot a = \begin{cases} 0_N & \text{if } a \notin N^* \\ \varphi_a(x) & \text{if } a \in \Phi(e_i) \text{and} \varphi_a(e_i) = a \end{cases}$$

The multiplication "$\cdot$" is well defined and moreover we get:

7.9. Theorem.

(a) Let $(N, +), |N| > 2$, be a finite group with a fixed point free automorphism group Φ. If "$\cdot$" is defined as in 7.8, then $(N, +, \cdot)$ is a planar nearring.
(b) Every finite planar nearring $(N, +, \cdot)$ can be constructed from a group $(N, +)$ and an appropriate fixed point free automorphism group Φ following Definition 7.8.

Proof. see [**Cla92**], p.45 to p.47. □

7.10. Proposition. Let Φ and Ψ be two conjugate fixed point free automorphism groups of the group $(N, +)$. Then for each nearring generated by Φ and N via Definition 7.8 there is an isomorphic nearring generated by Ψ and N.

Proof. Let $\alpha \in \mathrm{Aut}(N)$ such that $\Psi = \alpha^{-1}\Phi\alpha$. Suppose $e_i, 1 \leq i \leq m$, are the chosen orbit representatives for the nearring multiplication of $(N, +, \cdot)$ defined by Φ. It is easy to see that α^{-1} maps $(N, +, \cdot)$ to an isomorphic nearring $(N, +, \cdot')$ constructed by the representatives $\alpha^{-1}(e_i), 1 \leq i \leq m$ and Ψ. For $x \in N$ and $a \in N^*$ it holds

$$\alpha^{-1}(x \cdot a) = \alpha^{-1}(\varphi_a(x)) = \alpha^{-1}\varphi_a\alpha(\alpha^{-1}(x))$$

and $\alpha^{-1}\varphi_a\alpha =: \psi_{\alpha^{-1}(a)} \in \Psi$ such that $\psi_{\alpha^{-1}(a)}(\alpha^{-1}(e_i)) = \alpha^{-1}\varphi_a(e_i) = \alpha^{-1}(a)$. □

All non isomorphic planar nearrings with a given additive group N can be constructed from non conjugate fixed point free automorphism groups on N.

3. Finite Nearfields

Nearfields represent a vast matter in its own, although we are going to regard them simply as a special case of (planar) nearrings. Actually, it was the concept of nearfields which inspired the idea of nearrings. For an account of the theory of nearfields we refer to [**Pil83**] and [**Wäh87**].

7.11. Definition. A *nearfield* is a nearring $(N, +, \cdot)$ where $(N \setminus \{0\}, \cdot)$ is a group.

The structure of the additive groups of a nearfield is well known. As always we confine ourselves to the finite case.

7.12. Proposition. If $(N, +, \cdot)$ is a finite nearfield, then $(N, +)$ is elementary abelian.

Proof. see [**Pil83**], p.252. □

What is more:

7.13. Proposition. If $(N, +, \cdot)$ is a finite nearfield, then it is a planar nearring as long as $|N| > 2$.

Proof. see [**Cla92**], p.56. □

Thus nearfields on $(Z_p^n, +)$ are defined by fixed point free automorphism groups Φ on Z_p^n and vice versa by Theorem 7.9. In particular, $|\Phi| = p^n - 1$, that is, Φ is a fixed point free automorphism group of maximal size. This relation was actually used by Zassenhaus in [**Zas36**] to determine all finite nearfields. His investigation is based on the characterization of fixed point free automorphism groups in types (I) to (IV) as in Theorem 3.17 and non solvable ones as in Theorem 3.20.

Without prove we mention that the construction of a nearring multiplication on $(Z_p^n, +)$ with fixed point free maximal Φ according to Definition 7.8 provides a field for cyclic Φ, a so called *Dickson nearfield* for Φ of type (I) or quaternion Φ and one of 7 exceptional nearfields for the remaining cases. The 7 exceptions all have order p^2 with $p = 5, 7, 11$ (two cases), $23, 29$ or 59. See [**Pil83**], p.257, for a representation of them.

CHAPTER 8

An Implementation in GAP4

Now it is time for dessert: Actually constructing fixed point free automorphism groups on a given group G is a lot easier with the support of a computer. Straight forward algorithms turned out to be not very efficient, thus it seemed to be useful to implement all the knowledge gathered above. Even so, this should not be a purpose on its own but provide a tool to generate, e.g., Frobenius groups or planar near rings, objects which can be further investigated or manipulated to obtain, e.g., codes or designs see [**Cla92**] et al. So the outcome should not stand alone but be available within a larger computer algebra program. The functions described in the following are a small part of SONATA ("System Of Nearrings And Their Applications"), [**Tea97**], a share package based on GAP4 which was developed at the Institut für Algebra, Stochastik und wissensbasierte mathematische Systeme at the Johannes Kepler Universität Linz and funded by the "Fonds zur Förderung der wissenschaftlichen Forschung".

1. Preliminaries

First of all we introduce some basic features of the programming language GAP4. For details see the GAP4 reference manual and for a start in programming on your own see the GAP4 tutorial.

1.1. Objects.

Integers: `-2,0,1`.
Boolean Values: `true,false`.
Permutations: are written in cycle notation: `(1,2,3)` and `(1,2)(3,4)`.
Lists: are collections of objects separated by commas and enclosed in brackets: `[],[1..10],[a,b,c],[1,,3,,5]` and `[1,1,[1,2]]`. The i-th entry of a list `l` is accessible as `l[i]`.
Sets: are sorted lists without holes, i.e., lists all of whose entries are distinct and belong to the same type of object.
Matrices: are realized as list of lists.

1.2. Operators.

The operations `+,*,^-1`, etc., are generic, i.e., they can be applied to different types of objects, like integers, matrices, permutations, etc., whenever there is an appropriate meaning defined for that specific operation on the specific type of object. So `+` applied to integers or matrices means the usual addition, while `+` is not defined for permutations. Similarly, `*` is the usual multiplication for integers or matrices, for permutations it means applying one permutation after the other.

The operators `=,<>,<`, etc., test for equality, inequality, less than, and so on.

1.3. Domains.

A domain in GAP is a set of objects having an operational structure, i.e., a collection of operations under which the set is closed.

Groups, rings, fields, conjugacy classes of a group, etc., are domains. For example a group is closed under multiplication, taking the 0-th power and taking the inverse of elements.

Domains in GAP4 are objects and not records as in GAP3.

2. Defining Groups in GAP

In theory groups are abstract objects, whereas for computational purposes the specific representation of a group is important. The main types of representation are: pc groups, permutation groups, matrix groups and finitely presented groups.

We can realize a group by using generating elements in the form of permutations or matrices, by giving a presentation of generators and defining relations or by simply using a library of already implemented groups that comes with GAP.

We demonstrate these possibilities in case of the cyclic group of order 6 and the symmetric group on 3 points.

2.1. Pc group representations. Pc group stands for *polycyclic* group G, i.e., a group with a series

$$\{1_G\} = G_0 \lhd G_1 \lhd \cdots \lhd G_{n-1} \lhd G_n = G$$

in which each G_{i+1}/G_i is cyclic. In the finite case polycyclic is equivalent to solvable. Thus a solvable group has a polycyclic generating system $\{g_1, \dots, g_n\}$ such that $G_{i+1}/G_i = \langle g_{i+1} \cdot G_i \rangle$.

The GAP function `SmallGroup` retrieves a group of given size and number in the library of small groups with polycyclic generating system if solvable.

```
gap> Z6 := SmallGroup( 6, 2 );
<pc group with 2 generators>
gap> Z6 := CyclicGroup( 6 );
<pc group of size 6 with 2 generators>
gap> Z6 := AbelianGroup( [2,3] );
<pc group of size 6 with 2 generators>
gap> S3 := SmallGroup( 6, 1 );
<pc group with 2 generators>
```

2.2. Permutation group representations. A permutation groups can be easily realized by specifying its generators.

```
gap> Z6 := Group( (1,2,3,4,5,6) );
Group([ (1,2,3,4,5,6) ])
gap> Z6 := Group( (1,2),(3,4,5) );
Group([ (1,2), (3,4,5) ])
gap> S3 := SymmetricGroup( 3 );
Sym( [ 1 .. 3 ] )
gap> S3 := Group( (1,2),(2,3) );
Group([ (1,2), (2,3) ])
```

2.3. Matrix group representation.

```
gap> S3 := GL( 2, 2 );
SL(2,2)
```

2.4. Finite presentations. For a finite presentation of a group it is necessary to generate the free group with the appropriate number of generators, to define relations on this group and to factor the free group by the relations.

```
gap> F := FreeGroup( 1 );
<free group on the generators [ f1 ]>
gap> f := GeneratorsOfGroup( F );
[ f1 ]
gap> r := [f[1]^6];
[ f1^6 ]
gap> Z6 := F/r;
<fp group on the generators [ f1 ]>
gap> F := FreeGroup( 2 );
<free group on the generators [ f1, f2 ]>
gap> f := GeneratorsOfGroup( F );
[ f1, f2 ]
gap> r := [f[1]^2, f[2]^3, (f[1]*f[2])^2];
[ f1^2, f2^3, f1*f2*f1*f2 ]
gap> S3 := F/r;
<fp group on the generators [ f1, f2 ]>
```

3. Computation of Fixed Point Free Automorphism Groups

All the information gathered on fixed point free automorphism groups has been used to develop functions which compute all non conjugate fixed point free automorphism groups on an arbitrary given group G without using the straightforward approach of computing $\mathrm{Aut}(G)$ and searching for subgroups which operate on G in a fixed point free way. Since G has to be nilpotent, it suffices to compute on its p-Sylow subgroups S_p, which are direct factors of G, and to combine the results on each single S_p. Abelian subgroups S_p can even be replaced by a bunch of elementary abelian groups by Propositions 6.9 and 6.11 for computational purposes.

Furthermore, cyclic and quaternion fixed point free automorphism groups on abelian groups can be written down virtually immediately by the propositions given in Chapter 6. What remains is just a combinatorial problem to decide conjugacy. In the non abelian case a representative for each conjugacy class of $\mathrm{Aut}(S_p)$ is checked whether it generates a fixed point free automorphism group or not.

All groups of type (I) can be obtained by a single cyclic extension of a cyclic fixed point free automorphism group. If G is non abelian we are done. Otherwise by Theorem 3.12 groups of type (II) are computed by cyclic extension of groups H of type (I) with an element q such that $q^2 \in H$. According Theorem 3.15 Type (III) groups are realized as a semidirect product of the quaternion fixed point free automorphism group of order 8 which is unique by Proposition 6.27 and a type (I) group. Theorem 3.16 guarantees we just have to extend the type (III) groups by an element of order 4 and all solvable fixed point free automorphism groups on G are constructed.

If for each prime divisor p of $|G|$ the group $\mathrm{Aut}(S_p)$ contains a perfect subgroup of order 120 which operates on S_p in a fixed point free way, then the non solvable can be constructed via Theorem 3.20. Quite naturally, since each step is done on all invariant factors of G in parallel, the extension process stops as soon as it does not give a fixed point free automorphism group on one component.

The implementation of the procedures roughly described above heavily relies on the sophisticated algorithms for the computation of automorphism groups of p-groups, conjugacy classes and normalizers available in GAP4. The functions introduced in the following are part of the GAP4 share package SONATA.

We omit the source code and rather give a survey the main functions and their applications. Those interested in the whole truth can look up the program file "fpfaut.gi" that comes with SONATA.

3.1. IsFixedpointfreeAutomorphismGroup.

`IsFixedpointfreeAutomorphismGroup( phi, G )`

An automorphism group Φ of a group G is fixed point free if and only if every automorphism of Φ except the identity mapping has the group identity of G as the only fixed point, i.e., no element of G but the group identity is mapped onto itself.

The function `IsFixedpointfreeAutomorphismGroup` returns the according value `true` or `false` for a group of automorphisms `phi` on the group `G`.

```
gap> G := CyclicGroup( 11 );
<pc group of size 11 with 1 generators>
gap> g := GeneratorsOfGroup( G )[1];;
gap> phi := Group( GroupHomomorphismByImages( G, G, [g], [g^3] ) );
<group with 1 generators>
gap> Size( phi );
5
gap> IsFixedpointfreeAutomorphismGroup( phi, G );
true
```

3.2. FixedpointfreeAutomorphismGroups.

`FixedpointfreeAutomorphismGroups( G )`
`FixedpointfreeAutomorphismGroups( G, kmax )`

In the first form `FixedpointfreeAutomorphismGroups` returns a list of all groups of fixed point free automorphisms acting on the group `G` up to conjugacy.

In the second form `FixedpointfreeAutomorphismGroups` returns a list of all groups of size less then or equal to `kmax` of fixed point free automorphisms acting on the group `G` up to conjugacy. Note that a necessary condition for the existence of a fixed point free automorphism group `phi` on `G` is that the order of `phi` divides the order of `G` minus 1.

Note that the computation of all fixed point free automorphism groups even of a fixed size `k` may be rather time consuming if they are not cyclic. Conditions forcing a fixed point free automorphism group Φ to be cyclic are for example: $|\Phi|$ being the product of two not necessarily distinct primes, $|\Phi|$ being square free, $|\Phi|$ being an odd prime power or 2 times an odd prime power. Furthermore, Φ is cyclic if any of the Sylow subgroups of `G` is cyclic.

Otherwise `FixedpointfreeAutomorphismGroups` uses the function `FixedpointfreeAutomorphismGroupsByCyclicExtension` to compute representatives for all conjugacy classes of fixed point free subgroups of the automorphism group of `G`.

`FixedpointfreeAutomorphismGroups` calls the function `FixedpointfreeAutomorphismGroupsMaxSize`, also when `kmax` is given, to make sure `kmax` is a feasible order of a fixed point free automorphism group on `G`. If the size should not be checked, `FixedpointfreeAutomorphismGroupsNC( G, kmax )`

may be called.

```
gap> G := CyclicGroup( 11 );
<pc group of size 11 with 1 generators>
gap> G := CyclicGroup( 11 );;
gap> FixedpointfreeAutomorphismGroups( G );
[ <group of size 1 with 1 generators>,
  <group of size 2 with 1 generators>,
  <group of size 5 with 1 generators>,
  <group of size 10 with 1 generators> ]
gap> H := ElementaryAbelianGroup( 49 );;
gap> FixedpointfreeAutomorphismGroups( H, 24 );
[ <group of size 2 with 1 generators>,
  <group of size 3 with 1 generators>,
  <group of size 3 with 1 generators>,
  <group of size 4 with 1 generators>,
  <group of size 6 with 1 generators>,
  <group of size 6 with 1 generators>,
  <group of size 8 with 1 generators>,
  <group of size 8 with 2 generators>,
  <group of size 12 with 1 generators>,
  <group of size 12 with 2 generators>,
  <group of size 24 with 1 generators>,
  <group of size 24 with 2 generators>,
  <group of size 24 with 3 generators> ]
```

3.3. FixedpointfreeAutomorphismGroupsCyclic.

`FixedpointfreeAutomorphismGroupsCyclic( G )`
`FixedpointfreeAutomorphismGroupsCyclic( G, kmax )`

In the first form `FixedpointfreeAutomorphismGroupsCyclic` returns the list of all cyclic groups of fixed point free automorphisms acting on the group `G` up to conjugacy. In the second form `FixedpointfreeAutomorphismGroupsCyclic` returns the list of all cyclic groups of size less than or equal to `kmax` of fixed point free automorphisms acting on the group `G` up to conjugacy. Note that a necessary condition for the existence of a fixed point free automorphism group `phi` on `G` is that the order of `phi` divides the order of `G` minus 1.

`FixedpointfreeAutomorphismGroups` calls the function `FixedpointfreeAutomorphismGroupsMaxSize`, also when `kmax` is given, to make sure `kmax` is a feasible order of a fixed point free automorphism group on `G`. If the size should not be checked,

`FixedpointfreeAutomorphismGroupsCyclicNC( G, kmax )`

may be called.

```
gap> G := ElementaryAbelianGroup( 25 );;
gap> FixedpointfreeAutomorphismGroupsCyclicNC( G, 24 );
[ <group of size 2 with 1 generators>,
  <group of size 3 with 1 generators>,
  <group of size 4 with 1 generators>,
  <group of size 4 with 1 generators>,
  <group of size 6 with 1 generators>,
  <group of size 8 with 1 generators>,
  <group of size 12 with 1 generators>,
  <group of size 24 with 1 generators> ]
```

3.4. FixedpointfreeAutomorphismGroupsMaxSize.

`FixedpointfreeAutomorphismGroupsMaxSize( G )`

`FixedpointfreeAutomorphismGroupsMaxSize` returns a list with entries `kmax`, `metacyclic` and `quaternion` where `kmax` is an upper bound for the size of a fixed point free automorphism group on the group `G`; for example `kmax` divides the order of `G` and `kmax` is odd for nonabelian groups `G`. The order of any fixed point free automorphism group on `G` divides `kmax`.

The boolean `metacyclic` is `false` if there is no non cyclic fixed point free automorphism group on G such that all p-Sylow subgroups are cyclic and `true` if there could be one. The boolean `quaternion` is `false` if there is no quaternion fixed point free automorphism group on `G` and `true` if there is one. Thus, if both are `false`, then `G` has cyclic fixed point free automorphism groups only.

```
gap> H := ElementaryAbelianGroup( 49 );;
gap> FixedpointfreeAutomorphismGroupsMaxSize( H );
[ 48, true, true ]
gap> I := CyclicGroup( 15 );;
gap> FixedpointfreeAutomorphismGroupsMaxSize( I );
[ 2, false, false ]
```

3.5. FpfAutGrps.

`FpfAutGrps( G, metacyclic, quaternion, kmax )`

`FpfAutGrps` returns a list of all groups of size less then or equal to `kmax` of fixed point free automorphisms acting on the group `G` up to conjugacy. Thus `FpfAutGrps` does the same as the function `FixedpointfreeAutomorphismGroups` but one can determine individually whether metacyclic groups or groups with quaternion subgroup should be computed by setting `metacyclic` and `quaternion` equal to `true` or `false`, respectively.

If `metacyclic` or `quaternion` equals `true`, then the function `FixedpointfreeAutomorphismGroupsByCyclicExtension` is used.

```
gap> H := ElementaryAbelianGroup( 49 );;
gap> FpfAutGrps( H, true, false, 48 );
[ <group of size 2 with 1 generators>,
  <group of size 3 with 1 generators>,
  <group of size 3 with 1 generators>,
  <group of size 4 with 1 generators>,
  <group of size 6 with 1 generators>,
  <group of size 6 with 1 generators>,
  <group of size 8 with 1 generators>,
  <group of size 12 with 1 generators>,
  <group of size 12 with 2 generators>,
  <group of size 16 with 1 generators>,
  <group of size 24 with 1 generators>,
  <group of size 48 with 1 generators> ]
```

3.6. FixedpointfreeAutomorphismGroupsFieldGenerated.

`FixedpointfreeAutomorphismGroupsFieldGenerated( G, k )`

`FixedpointfreeAutomorphismGroupsFieldGenerated` returns a list with the field generated group of size `k` of fixed point free automorphisms acting on the elementary abelian group `G` as single entry.

A fixed point free automorphism group is *field generated* if there is a field $(F, +, .)$ such that `G` is isomorphic to the additive group of F and the generating automorphism is induced by multiplication with a specific element in the field.

```
gap> I := CyclicGroup( 9 );;
gap> FixedpointfreeAutomorphismGroupsFieldGenerated( I, 4 );
Error group not elementary abelian at
Error( "group not elementary abelian" );
<function>( <arguments> ) called from read-eval-loop
Entering break read-eval-print loop, you can 'quit;' to quit to\
 outer loop,
or you can return to continue
brk> quit;
gap> G := ElementaryAbelianGroup( 25 );;
gap> FixedpointfreeAutomorphismGroupsFieldGenerated( G, 4 );
[ <group of size 4 with 1 generators> ]
```

3.7. FrobeniusGroup.

`FrobeniusGroup( phi, N )`

`FrobeniusGroup` constructs the semidirect product of `N` with the fixed point free automorphism group `phi` of `N` with the multiplication $(f, n) \cdot (g, m) = (fg, g(n)m)$ by using the GAP function `SemidirectProduct`.

```
gap> N := AbelianGroup( IsPcGroup, [3,3,9,9] );
<pc group of size 729 with 6 generators>
gap> r := FixedpointfreeAutomorphismGroups( N );
[ <group of size 2 with 1 generators>,
  <group of size 4 with 1 generators>,
  <group of size 8 wit1h 1 generators>,
  <group of size 8 with 1 generators>,
  <group of size 8 with 2 generators> ]
gap>  phi := r[5];
<group of size 8 with 2 generators>
gap> F := FrobeniusGroup( phi, N );
<pc group with 9 generators>
```

CHAPTER 9

Examples of Special Fixed Point Free Automorphism Groups

To make the functions described above available, start GAP, type `RequirePackage( "sonata" );` and you will see the SONATA - banner appear. Note that this is the standard of December 1998, i.e., we are using SONATA 1b3 and GAP4b4. Both version and behavior of the following functions are bound to change with the ongoing development of GAP and SONATA. SONATA, a description, how to install it, and a manual is available from:

`http://www.algebra.uni-linz.ac.at/Sonata2/index.html`

1. Groups of Order 64

For a demonstration how the computer can be used to obtain examples in a convenient way, we choose to revisit a result by W.F. Ke and K.S. Wang who characterized the fixed point free automorphism groups on the groups of order 64 in [**KW93**]. They found out that there are only 7 non isomorphic groups of this size which admit a non trivial fixed point free automorphism group and 4 of them are abelian. An explicit representation of these groups and of the automorphisms was given.

We use the standard GAP functions as well as the functions described above that come with SONATA. I am indebted to Bettina Eick and E. A. O'Brien for their package AutPGrp [**EO**] which reduces the time for the computation of the automorphism group of a finite p-group considerably. While it is not necessary for SONATA to work, we recommend its use, when you deal with automorphism groups of non abelian groups. We type

```
gap> RequirePackage( "autpgrp" );
 Computing automorphism groups of p-groups
```

to have these functions at hand.

First of all we determine the total number of non isomorphic groups of size 64. Up to order 1023, all groups are available in a library with the exception of the groups with 512 elements.

```
gap> NumberSmallGroups( 64 );
267
```

Instead of looping over all 267 groups and trying to compute a fixed point free automorphism group thereupon, we first exclude those which cannot admit such automorphisms. We operate with lists and functions on lists.

```
gap> l := List( [1..267], x ->
>       [x, FixedpointfreeAutomorphismGroupsMaxSize(
>              SmallGroup( 64, x ) )[1]] );;
```

```
gap> time;
10370
gap> l := Filtered( l, x -> x[2] > 1 );
[ [ 2, 3 ], [ 23, 3 ], [ 55, 7 ], [ 76, 7 ], [ 79, 7 ], [ 81, 7 ],
  [ 82, 7 ], [ 192, 3 ], [ 217, 3 ], [ 220, 3 ], [ 223, 3 ],
  [ 224, 3 ], [ 227, 3 ], [ 231, 3 ], [ 238, 3 ], [ 239, 3 ],
  [ 241, 3 ], [ 242, 3 ], [ 245, 3 ], [ 267, 63 ] ]
gap> Length( l );
20
```

We have 20 candidates G left which could have a non trivial fixed point free automorphism group Φ. The command `time` gives the information that it took 10370 milliseconds to apply `FixedpointfreeAutomorphismGroupsMaxSize` on all 267 groups. `l` is now a list of pairs where the first component describes the number of G in the library of small groups, the second is an upper bound for the size of Φ fixed point free on G. We note that $|\Phi|$ is either less than 3 or less than 7, only for the group with number 267 a Φ of order 63 could not be excluded. Indeed, `SmallGroup( 64, 267 )` is the elementary abelian group.

```
gap> Gs := List( l, x -> SmallGroup( 64, x[1] ) );;
gap> phis := List( [1..20], i ->
>       FixedpointfreeAutomorphismGroupsNC( Gs[i], l[i][2] ) );
[ [ <group of size 3 with 1 generators> ], [  ],
  [ <group of size 7 with 1 generators> ], [  ], [  ], [  ],
  [ <group of size 7 with 1 generators> ],
  [ <group of size 3 with 1 generators> ], [  ], [  ], [  ],
  [  ], [  ], [  ], [  ], [  ], [  ],
  [ <group of size 3 with 1 generators> ],
  [ <group of size 3 with 1 generators> ],
  [ <group of size 3 with 1 generators>,
    <group of size 7 with 1 generators>,
    <group of size 7 with 1 generators>,
    <group of size 9 with 1 generators>,
    <group of size 21 with 1 generators>,
    <group of size 63 with 1 generators>,
    <group of size 63 with 2 generators> ] ]
gap> time;
63390
gap> Number( phis, x -> x <> [] );
7
```

Thus there are 7 groups remaining with a non trivial automorphism group. It took 63 seconds to find all of them.

```
gap> l := ListX( [1..Length( phis )], i -> phis[i] <> [],
>                                            i -> l[i] );
[ [ 2, 3 ], [ 55, 7 ], [ 82, 7 ], [ 192, 3 ], [ 242, 3 ],
  [ 245, 3 ], [ 267, 63 ] ]
gap> Gs := ListX( [1..Length( phis )], i -> phis[i] <> [],
>                                            i -> Gs[i] );;
gap> List( Gs, IsAbelian );
[ true, true, false, true, false, false, true ]
```

We see that the groups of order 64 with numbers 2 and 192 in the `SmallGroup`-library both are abelian and have a fixed point free automorphism group of order 3. They are isomorphic to Z_8^2 and $Z_4^2 \oplus Z_2^2$ respectively. Group number 55 is isomorphic to Z_4^3 and has a Φ with size 7. Of course, the elementary abelian group with number 267 admits Φ with orders up to 63.

There are 3 non abelian groups left; number 82 is called $A(3, \vartheta)$ in [**KW93**] and has a fixed point free automorphism group of order 7, numbers 242 and 245 corresponding to $\mathcal{T}$ and $\mathcal{S}$ respectively both have Φ of order 3.

It is easy to see that no non abelian group of cardinality less than 64 can have a non trivial fixed point free automorphism group.

2. The Elementary Abelian Group of Order 121

We take a look at the fixed point free automorphism groups of Z_{11}^2.

```
gap> G := ElementaryAbelianGroup( 121 );
<pc group of size 121 with 2 generators>
gap> phis := FixedpointfreeAutomorphismGroupsNC( G, 120 );
[ <group of size 2 with 1 generators>,
  <group of size 3 with 1 generators>,
  <group of size 4 with 1 generators>,
  <group of size 5 with 1 generators>,
  <group of size 5 with 1 generators>,
  <group of size 5 with 1 generators>,
  <group of size 6 with 1 generators>,
  <group of size 8 with 1 generators>,
  <group of size 8 with 2 generators>,
  <group of size 10 with 1 generators>,
  <group of size 10 with 1 generators>,
  <group of size 10 with 1 generators>,
  <group of size 12 with 1 generators>,
  <group of size 12 with 2 generators>,
  <group of size 15 with 1 generators>,
  <group of size 20 with 1 generators>,
  <group of size 20 with 2 generators>,
  <group of size 24 with 1 generators>,
  <group of size 24 with 2 generators>,
  <group of size 24 with 3 generators>,
  <group of size 30 with 1 generators>,
  <group of size 40 with 1 generators>,
  <group of size 40 with 2 generators>,
  <group of size 60 with 1 generators>,
  <group of size 60 with 2 generators>,
  <group of size 120 with 1 generators>,
  <group of size 120 with 2 generators>,
  <group of size 120 with 3 generators>,
  <group of size 120 with 3 generators> ]
gap> time;
65300
```

The answer was returned after a little bit more than a minute. Note that there are in total 4 fixed point free automorphism groups of order 120: one cyclic, corresponding to the field $GF(121)$, one non cyclic of type (I), corresponding to the Dickson nearfield, one of type (III) and a perfect one, isomorphic to $SL(2, 5)$, which define the remaining two nearfields of order 121.

3. An Abelian Example

In Chapter 7 we gave fixed point free automorphism groups of the group $Z_5^4 \times Z_{49}^2$ as an example. We will check the results given there by using SONATA:

```
gap> G := AbelianGroup( [ 5, 5, 5, 5, 49, 49 ] );
<pc group of size 1500625 with 8 generators>
gap> phis := FixedpointfreeAutomorphismGroupsNC( G, 16 );
[ <group of size 2 with 1 generators>,
  <group of size 4 with 1 generators>,
  <group of size 4 with 1 generators>,
  <group of size 4 with 1 generators>,
  <group of size 4 with 1 generators>,
  <group of size 8 with 1 generators>,
  <group of size 8 with 1 generators>,
  <group of size 8 with 2 generators>,
  <group of size 16 with 1 generators>,
  <group of size 16 with 2 generators> ]
gap> time;
69780
```

The answer corresponds to what we obtained by the calculations by hand. Up to conjugacy there are 2 cyclic fixed point free automorphism groups of order 8, and 1 of order 16, as well as 1 quaternion group of order 8 and 1 of order 16. The relatively long computational time of 69 seconds is almost completely due to the transfer from the internal representation of the mappings to the GAP representation of automorphisms on the group.

Lebenslauf

Am 1.5.1974 wurde ich als Sohn von Eduard und Maria Mayr geboren. Von 1980 bis 1984 besuchte ich die Volkschule in Traun-Oedt, anschließend den naturwissenschaftlichen Zweig des Bundesrealgymnasiums Traun, wo ich im Juni 1992 die Reifeprüfung mit ausgezeichnetem Erfolg abschloß.

Im Oktober 1992 begann ich mit dem Studium der Technischen Mathematik und parallel dazu mit dem der Technischen Physik. Die Mathematik beanspruchte immer mehr mein Interesse und im Juni 1995 beendete ich den ersten Studienabschnitt mit Auszeichnung. Nunmehr war Technischen Mathematik, Studienzweig Mathematik in den Naturwissenschaften, meine Hauptstudienrichtung.

Seit Juni 1997 arbeitete ich am von Prof. Dr. Günter Pilz geleiteten Projekt mit dem Titel "SONATA" in den Bereichen planare Fastringe, wd-Fastringe und Designs mit. Von Oktober 1997 bis Oktober 1998 leistete ich Zivildienst, anschließend erhielt ich für meine Teilnahme an SONATA eine Forschungsbeihilfe vom "Fonds zur Förderung der wissenschaftlichen Forschung".

Bibliography

[AW92] William A. Adkins and Steven H. Weintraub. *Algebra. An Approach via Module Theory*, volume 136 of *Graduate Texts in Mathematics*. Springer Verlag, New York, 1992.

[Cla92] James R. Clay. *Nearrings. Geneses and Applications*. Oxford University Press, Oxford, New York, Tokyo, 1992.

[EO] Bettina Eick and E. A. O'Brien. Autpgrp – share package of gap 4. Available from: http://www.mathematik.uni-kassel.de/ eick/.

[HB82] Bertram Huppert and Norman Blackburn. *Finite Groups III*, volume 243 of *Grundlehren der mathmatischen Wissenschaften in Einzeldarstellungen - A Series of Comprehensive Studies in Mathematics*. Springer Verlag, Berlin, Heidelberg, 1982.

[Hup67] Bertram Huppert. *Endliche Gruppen I*, volume 134 of *Die Grundlehren der mathmatischen Wissenschaften in Einzeldarstellungen*. Springer Verlag, Berlin, Heidelberg, 1967.

[KK95] Wen-Fong Ke and Hubert Kiechle. Characterization of some finite ferrero pairs. In *Near-Rings and Near-Fields*, volume 336 of *Mathematics and Its Applications*, pages 153–160. Kluwer Academic Publishers, Dordrecht, Boston, London, 1995. Proceedings of the Conference on Near-Rings and Near-Fields, Fredericton, New Brunswick, Canada, July 18-24, 1993.

[KW93] W.F. Ke and K.S. Wang. *On the Frobenius Groups with Kernel of Order 64*, volume 7 of *Contributions to General Algebra*, pages 153–160. Hölder Pichler Tempsky, Wien, 1993.

[LN84] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Springer Verlag, New York, 1984.

[Pil83] Günter Pilz. *Near-Rings. The Theory and its Applications*, volume 23 of *North-Holland Mathematics Studies*. North-Holland Publishing Company, Amsterdam, New York, Oxford, revised edition, 1983.

[Rob96] Derek J. S. Robinson. *A Course in the Theory of Groups*, volume 80 of *Graduate Texts in Mathematics*. Springer Verlag, New York, second edition, 1996.

[Tea97] The SONATA Team. *SONATA: Systems Of Nearrings And Their Applications*. Universität Linz, Austria, 1997. Available from: http://www.algebra.uni-linz.ac.at/Sonata2/index.html.

[Wäh87] Heinz Wähling. *Theorie der Fastkörper*. Thales Verlag, Essen, 1987.

[Wol67] Joseph Albert Wolf. *Spaces of Constant Curvature*. McGraw-Hill, New York, 1967.

[Zas36] Hans Zassenhaus. *Über endliche Fastkörper*, volume 11 of *Abhandlungen aus dem Mathematischen Seminar der Univesität Hamburg*, pages 187–220. 1936.

[Zas85] Hans Zassenhaus. *On Frobenius Groups I*, volume 8 of *Results in Mathematics*, pages 132–145. 1985.

Index

abelian invariants, 4
annihilator, 11
automorphism, 1
  inner, 1
automorphism group, 1
  fixed point free
    cyclic, 34, 56
    non solvable, 29
    number of, 39, 46, 57
    of a cyclic group, 31
    of an abelian group, 52
    perfect, 29
    quaternion, 42, 43, 59
    solvable, 28
  of a cyclic group, 4
  inner, 2
AUTPGRP, 75

block matrix, 15

center, 2
centralizer, 2
characteristic polynomial of a linear transformation, 14
characteristic subgroup, 2
commutator, 6
companion matrix, 15
complement, 3
conjugate, 1
cyclotomic field, 36

derived subgroup, 6
dihedral group, 7
direct product, 3

eigenvalue, 12
eigenvector, 12
elementary divisors of a linear transformation, 14
endomorphism, 1
epimorphism, 1
Euler's function, 4

fixed point, 3
fixed point free
  automorphism, 3
  automorphism group, 3
  linear transformation, 12
Frattini subgroup, 9
Frobenius complement, 61
Frobenius group, 61
Frobenius kernel, 61
fully invariant subgroup, 2

GAP4, 67
general linear group, 9
Grüns theorem, 10
group
  of type (I), 21, 28
  of type (II), 22, 28
  of type (III), 24, 28
  of type (IV), 26, 28

homomorphism
  of a group, 1
  of an R-module, 11

image of a homorphism, 1
invariant factors of a linear transformation, 14
isomorphism, 1
isomorphism theorem
  first, 2

kernel of a homorphism, 1

linear transformation, 12

Maschke, Schur theorem, 49
metacyclic group, 22
minimal polynomial of a linear transformation, 14
monomorphism, 1

nearfield, 65
  Dickson, 65
nearring, 63
  planar, 64
nilpotent group, 7
normal subgroup, 2

order of a polynomial, 16

p-group, 3
perfect, 6
polycyclic group, 68
primary R-module, 14

quaternion group, 7
  properties of, 7–8

R-module, 11
rational canonical form, 15

Schur-Zassenhaus theorem, 9
semidihedral group, 7
semidirect product, 3
solvable group, 6
SONATA, 67
special linear group, 9
Sylow subgroup, 3
Sylow theorems, 3

Thompson's theorem, 19
torsion element, 11
torsion module, 11

vector space, 12

Z_n^*, 4